HELSINKI SCHOOL OF ECONOMICS (HSE)
Department of Accounting and Finance

ELEMENTS OF FRAUD COSTS

Finance
Master´s thesis
Olli Pitkänen
Fall 2007

Approved by the Council of the Department 27 / 11 2007 and awarded the grade hyvä, 60 pistettä

Tarkastajat:
KTT, Vesa Puttonen ja
KTT, Sami Torstila

Helsinki School of Economics

Master's Thesis
Olli Pitkänen

Abstract

November 7, 2007

ELEMENTS OF FRAUD COSTS

PURPOSE OF THE STUDY

The goal of this study is to examine how significant companies regard fraud risk, where the damages arise from and how the risks can be prevented. Focus is in the three sources of total fraud cost, which are related to risks, prevention and recovery. Results can be used to enhance companies' risk management practises and thus contribute to the value creation.

DATA

Data for this study was acquired from five face to face interviews. During 2006 six risk management experts from three public companies and two government agencies in Finland were interviewed. Interviewees are risk and security managers or head of internal audit. Interview constituted from 29 open end questions divided into fours subgroups.

RESULTS

Companies regard fraud as a significant risk. It is typically related to non-monetary, intangible items, such as reputation, image or customer relationships. Fraud risk is difficult to transfer because of its intangible nature. Most significant risk is reputation risk as it can endanger the existence of the business. Estimated damages vary from 10 to 100 million euro. Indirect costs are stated to be even more than direct costs in some fraud cases. Fraud risk management concentrates into high risk areas through the use of various methods, such as system built in security controls, training and guidance or specific risk area reviews. Companies are preparing for future risks, such as international criminality, by implementing enterprise wide risk management practises, through information management and information technology system improvements.

KEYWORDS

Fraud, risk management, fraud cost.

Helsingin kauppakorkeakoulu **Tiivistelmä**

Pro gradu -tutkielma **7.11.2007**
Olli Pitkänen

TALOUDELLISTEN VÄÄRINKÄYTÖSTEN KUSTANNUSELEMENTIT

TAVOITE

Tutkimuksen tavoitteena on selvittää miten merkittävänä uhkana yritykset pitävät taloudellisia väärinkäytöksiä, mistä vahingot syntyvät ja kuinka riskejä ennaltaehkäistään. Tutkimuksessa tarkastellaan väärinkäytösten kokonaiskustannuksia riskeihin, ennaltaehkäisyyn ja vahinkojen palauttamisen kannalta. Tuloksia voidaan käyttää parantamaan riskienhallintamenetelmiä ja näin ollen lisäämään yrityksen arvoa.

AINEISTO JA MENETELMÄT

Tutkimuksen aineisto perustuu viiteen haastatteluun. Vuoden 2006 aikana kuutta riskienhallinnan ammattilaista haastateltiin kolmesta pörssiyhtiöstä ja kahdesta julkisen sektorin toimijasta. Haastatellut ovat riskienhallinta-, turvallisuus- tai sisäisen tarkastuksen johtajia. Haastattelu sisälsi 29 avointa kysymystä, jotka olivat jaettu neljään ryhmään.

TULOKSET

Yritykset pitävät taloudellisia väärinkäytöksiä merkittävinä riskeinä. Ne liittyvät tyypillisesti aineettomiin asioihin, kuten maineeseen, imagoon tai asiakassuhteisiin. Riskejä on vaikea siirtää niiden aineettoman luonteen takia. Merkittävin väärinkäytösriski on maineriski, koska se voi uhata koko yrityksen olemassaoloa. Arvioidut vahingot vaihtelevat 10:stä 100 miljoonaan euroon. Epäsuorien kustannuksien todettiin nousevan suoria kustannuksia suuremmiksi joissain tapauksissa. Riskienhallinta keskittyy isoihin riskeihin käyttämällä erilaisia menetelmiä, kuten järjestelmien sisäisiä turvallisuuskontrolleja, koulutusta ja ohjeistusta tai erityisiä riskialueiden tarkastuksia. Tulevaisuuden riskeihin, kuten kansainväliseen rikollisuuteen, varaudutaan implementoimalla ERM-järjestelmä, tiedonhallinnalla ja IT-järjestelmillä.

AVAINSANAT

Taloudellinen väärinkäytös, riskienhallinta, taloudellinen väärinkäytöskustannus.

Table of contents

1. Introduction

This study shows the elements of fraud costs from the practical point of view. It points out how Finnish companies and public sector agencies regard fraud risk, what kind of damages fraud can cause to the companies and to the public sector agencies and how the companies and public sector agencies are preparing for the fraud risks, if at all. The data is gathered from the face to face interviews of risk management practitioners. The focus is in the three sources of costs, namely in risks, prevention and recovery. These sources of fraud costs are in order based on the time when costs arise. First of all, risks form the basis of this issue, causing potential costs to the entities. Secondly, after recognizing the risks and analysis of the threat, entities can try to prevent the risks. Preventive methods cause costs to the entity. Finally, if the fraud risk realizes and causes damages to the entity, they can recover fully or partly from the incident. This breakdown of the sources of fraud cost and the interrelations are discussed in this study.

1.1. General background and motivation

In the financial crime literature the term fraud contains various crimes and is not seen only as a "white-collar" crime. The term 'White-collar criminal' was first mentioned by Edwin Sutherland in his speech on 27 of December 1939 to the American Sociological Association. Today the areas of interest covering or relating to fraud vary from corruption, environmental crime, pharmaceutical fraud, tax fraud, money laundering and public sector fraud to insurance fraud, pensions mis-selling, banking fraud, corporate fraud, financial fraud and organisational crime. Even though the list is not complete it shows that fraud and corruption has many forms. The problem of fraud and corruption is widespread and exists everywhere regardless of the country, industry or culture. This can be seen for example from the results of Transparency International corruption indices, which cover most of the countries in the world. None of the countries is completely clean from corruption. Nordic countries have been considered as uncorrupted and Finnish business people are valued honest according to Transparency International (2007). It is true that there are regional differences and fraud can be industry specific, but the underlying logic of fraud and corruption states that most likely they are found in the neighbourhood of money and other capital. Even though this argument sounds obvious, it is often neglected and thus can lead to unexpected issues. This paper intends to shed light on how Finnish companies see the fraud risk and how significant it is regarded.

To get a view of the scale of this phenomenon, we can look to the estimated aggregate losses amounting from frauds. According to the Report to the Nation on Occupational Fraud and Abuse (2002) the fraud examiners estimate that corporations lose about 6 % of their revenue due to occupational fraud and abuse. This amounts to $ 600 billion in 2002 in U.S. and compared to the 1996 figure of $ 400 billion, there is a 50 % increase in this period. The average loss of revenue in U.S. is huge compared for example to the net profit margins. Similar kind of study has not been prepared with Finnish data. Thus one of the goals of this study is to clarify what kind of damages fraud can cause to Finnish companies.

Who is then committing fraud? The possible fraudster can be almost anyone as long as there is opportunity and motivation to commit a fraud and there is a perception that you are not going to get caught according to Albrecht and Wernz (1993). Certain factors, such as position, gender, age, education, collusion and criminal history in the perpetrator profile affect to the size of the losses according to the Association of Certified Fraud Examiners' (ACFE) report (2002). These findings are used in formulation of the interview questions regarding fraud prevention. Intention is to go through the methods Finnish companies use in fraud prevention.

There are some explanations why corporations engage into criminal activities. Cloninger (1982) suggest a general hypothesis that agents may resort to illegal or unethical activity as additional means of enhancing share price. Furthermore, Reichert, Lockett, and Rao (1996) argue that agents use illegal activities that market perceives as speculative and destabilizing to the firms returns. However, Cloninger and Waller (2000) argue that the speculative hypothesis is only a special case of hedging hypothesis.

According to the empirical evidence of Cloninger and Waller (2000) there are two viable hypotheses why corporations engage in criminal activity. The most referred hypothesis is the Rotten Apple Theory or agency problem, which states that fraudulent activity is an outcome of a few scrupulous agents. Another, the hedging hypothesis, argues that some agents pursue illegal activities in order to enhance the share price. Cloninger states that both of these agents coexist. He argues that asymmetric information provides agent with opportunity to fraudulent activity and the share price maximisation goal provides the motive. Hence, he suggests that the goal of share price maximisation should be replaced with stakeholder value maximisation to provide managers with goals, which are consistent with ethical standards. Additionally to

these hypotheses of corporation engaging criminal activity, sociological literature introduces plenty of other motives and reasons for crime and fraudulent activity. These are introduced in the chapter 2.5. Criminal motivation theories.

Interest to research fraud started to arouse among the academics after Sutherland introduced his famous white-collar criminality paper in 1940. However, it has taken a long time to become a recognized issue. Krambia-Kapardis (2002) summarised many reasons for this, such as poor knowledge, inadequate statistics, lack of theory and research, and difficulties in control. She states that there are problems in recording the corporate offences and even greater problems when trying to assess the costs of the offences. Thus there has not been good enough tools to gather information, evaluate it and manage it properly. This paper introduces the elements of fraud costs to companies, thus it helps the process of developing fraud management tools.

This topic is challenging in many ways. First of all, it covers many areas of interests, such as economics, finance, sociology, law, criminology and psychology. Secondly, research carried out in this field is limited, mainly concentrating in financial frauds and auditors' responsibility, tax frauds or banking and insurance fraud schemes. The cost of fraud in many studies or surveys is neglected because it is perceived difficult to measure and assess. There are some studies concentrating on the evaluation of fraud cost from news headlines and share prices, such as Master's thesis of Heiskanen (2006). However, the purpose of this study is to look deeper into the actual fraud cost elements and thus give more information about the division of the total cost of fraud.

1.2. Research problem and goals of the study

The goals of this study are to examine how significant companies regard fraud risk, where the damages arise from and how the risks can be prevented. Focus is in the three sources of total fraud cost, which are related to risks, prevention and recovery. This division of the costs in this study is based on the time when costs occur. Risks arise first, then companies try to prevent the risks and finally, if not succeeding doing so, trying to recover from the damages. Significance of the fraud is examined through the risk recognition, treatment, and fraud prevention training provided. Risk prevention is observed through the tone at the top, use of controls, follow-up, monitoring and detection processes. Risks and damages are looked closer through companies' risk assessment process. Level, area and scale of the assessment process

are investigated. Management of the fraud risk and recovery is further investigated through incident management, availability of the response plan and investigation team, as well as sanctions and follow up processes. Results can be used to enhance companies' risk management practises and thus contribute to the company value creation.

1.3. Contribution and perspectives

There are some studies concentrating on the fraud and corruption news and share prices and several fraud and corruption victimisation studies as well as explanatory studies of the economic crime reasons. The contribution of this study, however, is to introduce the breakdown of the total fraud cost called fraud costs elements. The breakdown of the costs enables the differentiation of the costs and thus improves the understanding of the costs. As well, this study shows the interrelations of the different kind of fraud and corruption costs.

The perspective of the study is practical oriented and only from company's point of view. This is to improve the applicability of the results to risk management practise. Data is gathered from face to face interviews from subject matter experts, who are practising fraud and corruption prevention in their daily job. Hands on attitude are reflected in the answers of the practitioners.

1.4. Limitations

Focus of this research is on Finland based companies and government agencies, thus the results may not be fully generalized to the international context. Nature of this study is descriptive. Number of interviews is limited to five, which enables to concentrate on the insights of these selected interviewees, who are experts in the security, risk management and internal audit. Due to selection of the interviewees and many open questions, this study does not allow conducting proper statistical analysis; however, the results act merely as guidance. This paper concentrates only to companies and thus does not take into account fraud and corruption to the third parties, such as government or general public.

1.5. Structure of the study

Five chapters form the structure of this paper. This paper starts with an introductory chapter and continues to the literature review. Following third chapter goes through the types of fraud and corruption costs as well as comparison of these types. Fourth chapter includes discussed the methodology used in this paper and continues then to the data and analysis. Conclusions

are presented in the fifth chapter with the future research suggestions. References can be found after conclusions and future research chapter. Appendix includes the interview questionnaire and it is shown after the references. Index of tables presented in this study is summarized in the end of this paper.

2. Literature review

2.1. Economic crime, fraud and corruption

The basis of the fraud discussion is found in the criminology and more specifically in the area of economic crime or under a notion of white collar crime. There are, however, some problems in approaching this phenomenon. There are three sets of ambiguities related to this subject according to the Slapper and Tombs (1999); firstly the definition problem, secondly the causes of economic crime and thirdly the regulation and handling of economic crime. This chapter starts by introducing the definition problem, which some people regard as the most important one, and then continuing to the possible causes of crime and finally introducing the regulation and handling of economic crime.

Not just the definition of economic crime, but the definition of crime in general varies in different cultures and from time to time. There are several ways to approach crime and thus, for example, criminals have been seen as heroes, villains, fools, revolutionaries, deviants and scumbags in people's mind. The common definitional approaches to a crime are legalistic by Tappan (1947), conduct norms by Sellin (1938), social harm by Sutherland (1949), human rights violation by Schwendingers (1975), deviance and social control, social problem and chaos approaches. These various approaches to crimes and especially to economic crimes make the common definition of the concepts difficult.

Specifically what comes to the definitional problems of economic crime, it is not clear what areas of crimes are included in the concept of economic crime. The variety of the possible economic crimes include the following and more: white collar criminality, environmental crime, corporation crime, business crime, occupational crime, antitrust, banking, financial, insurance, telemarketing, accounting, tax and health and safety frauds, cyber crime, organized crime, terrorism, customs violations, bribery, gratuities, corruption, money laundering, identity thefts, larceny, perjury, forfeiture, embezzlement, espionage, conspiracy, regulatory crimes, extortion and violence against employees. Some of these terms are overlapping or subgroups of another; however, this list shows the diversity of the possible crime types.

As well the academic considerations of behaviour categorized as a crime is in some parts

controversial to the crime concept in the legal or sociological setting. As mentioned before, there are several approaches to the notion of economic "crime" conduct, which is not criminalized by the law. The legalistic approach introduced by Tappan (1947) regards only conduct, which is criminalized by the law as an economic crime. Sociological approaches, however, treats also deviant acts violating some informal norm as an economic crime. This deviant activity does not need to be criminalized by the crime or civil law currently, but it drives the concerns of reforming the law.

There are various, conflicting, and overlapping ways to see the economic crime, the perpetrators and the act of crime. Theorists often claim economic crime has some special characteristics differentiating it from other types of crimes. What defines economic crime is not a well-defined collection of common properties, but instead a set of resemblances, series of similarities and relationships shared by the class.

Economic crime is said to differentiate from other types of crimes by not being easy to measure, unless using appropriate methods and looking into the right area. Generally economic crimes takes place in a private setting, thus this might facilitate the commission of crime. Therefore economic crime is invisible in that sense that it does not have direct consequences in a specific date or location. As well, target of economic crimes can be intangible and offenders can be only partly responsible of the whole act. Thus it is not as easy to pinpoint an economic crime offence as an ordinary crime, where the act of crime can be said to happen in a certain place by a certain actor and with a real object missing. Often the effects of economic crime offences can be felt much later than the act or series of acts of crime and what is more, the effects are unlikely to be attributed to the crime.

Offenders are usually part of the middle or high class in society; they are members of the respectable group and are not in dire need of money. Thus perpetrators have a lot to lose, that is their reputation, family ties, career and wealth. Perpetrators motivation of committing economic crimes can be related to the changes of being caught. Changes being caught are relatively lower than in ordinary crime, because economic crimes are not expected to happen and thus we are not looking for them. Therefore perpetrators perceived risk to getting caught is seen smaller and this lowers the threshold to become a criminal. Because offenders are typically in a relatively powerful position in their company or in society, they usually have various measures to hide their traces of fraud and corruption.

The costs and damages, even including violence and death, related to the economic crimes are usually much higher than in conventional crime according to the Slapper and Tombs (1999: 54-84). However, the direct link between economic crimes and costs is harder to see because of the several factors, such as expertise and position needed to do the act of economic crime, time the offence might take and time that takes to recover from the incident. As well, indirect cost effects are thought to be even larger than direct consequences from fraud and corruption.

Second set of ambiguities is about the theories of the possible causes of economic crime. Some scholars apply the general criminological frameworks to the economic crimes, while others doubt this approach claiming that offender behaviour takes place in a more respectable context than most of the other crimes and has more ambiguous intentions than common crimes. The common criminological theoretical framework includes varying theories for example from biological, psychological, social disorganization, anomie, social learning, control, labelling, radical conflict, feminist, middle-class and integrated approaches. Even though these theories enlighten some aspects of human behaviour in general, they are still not fully adequate theories to explain economic crime or deviances.

Possible candidates for origin of crime are suggested to be poverty, careless reproduction, disorderly families, inequalities of wealth and power, inadequate schooling, insufficient working possibilities, the low probability of punishment, heterogeneous population, welfarism and its corruption of individual responsibility, racist, sexist and classist messages broadcast by the entertainment and information industries, etc. However, none of these nominees is, first of all, well defined and secondly, known to have specific causal interrelation to the crimes according to the Nettler (1991). There are so many different forms of economics crimes and known motivations that it is quite obvious that there is no single explaining factor, which would be accused to cause an economic crime. It is a complex problem, as well as human behaviour in general.

Third set of ambiguities refers to the ambivalent ways to regulate and handle economic crime. From psychological point of view, it is hard to see "the criminal" and "the respectable person" in one and the same figure. Nevertheless, this is usually the case in the economic crime offences. Perpetrators typically have a very good social status thus it could be difficult to understand the motives and reasoning behind the act. Because respectable member of the

society can be seen as heroes or role models, convicting them can be seen as a shock from the public point of view, which in turn might erode common morale.

There is a danger that economic crime is treated differently compared to the other kind of crime because of the higher status of the perpetrators. Taking this into extreme, different attitudes could lead to different laws for the elite and for the commons. This would be against the principles of democracy and law, which is the basis of our modern society. In order to treat economic crimes equal to other types of crime they need to be part of the normal police property. Economic crimes have become part of the normal police property in Finland not until the last decade according to Alvessalo and Tombs (1994), thus it is quite a new issue. Before that there had merely been a discussion over the importance of the economic crimes in the official crime statistics. Because economic crimes were not treated as a normal crime, they were not included in the statistics and thus there were not an adequate basis for the discussion. Economic crimes have been included in the statistics not until recently and there are still differences in the definitions and measures. These differences make it harder to compare various statistics and make sound conclusions about the changes in economic crime trends and the effectiveness of the measures. As well, there are many reasons why statistics have not included economic crimes or why they have been included only partly.

One main reason is that economic crime against the companies is not separately compiled to the statistics in Finland. Secondly, the nature of crime is hidden and thus most of the economic crime does not come the knowledge of law enforcement agencies, because there is no obligation for companies based on law to report any economic crime incident. According to the report of Keskuskauppakamari (Central Chamber of Commerce, Finland) and Helsingin Kauppakamari (Helsinki Chamber of Commerce) (2005), most of the crime against the companies stays hidden. As well, laws have changed and become tighter, because of the world scale corporate scandals as Enron, Worldcom and Parmalat have shown. Therefore statistical data does not only reflect changes in the crime trends, but also changes in the control of crimes, changes in law, as well as changes in willingness to report crimes.

2.2. Definitions, fraud

Fraud, as well as corruption, is a part of the economic crime. The concept of economic crime was introduced first by Edwin Sutherland (1940), defining “white collar crime” as a "crime committed by a person of respectability and high social status in the course of his

occupation." He disregarded the concept of crime defined by the crime law and expanded economic crimes including injustices also in the civil law and administrative law. Currently the meaning of the economic crime varies among practitioners and researchers depending on their point of view. Thus a discussion is still going on what should be included in the concept of economic crime. For example Sutherland's injustices are still under discussion as well as the question of what kind of damaging, including economic, physical and social, acts should be defined to include in an economic crime (Alvessalo and Tombs, 1994). The variety of definitions can lead to a poor comparability of studies as well as to the compatibility of the risk management practises. As can be seen, sometimes same offences are categorised under the notion of fraud or corruption, sometimes they are treated as economic crimes or something similar. This might be because of the use of different definitions or because offences include various elements of fraud, corruption and economic crime. Even though definitions are partly or totally overlapping, they enlighten the scale of possible offences. Definitions are important for the identification and measurement purposes, but also for the communication of the rules in the corporation, sometimes interpreted in different ways. As well, definitions are important for the comparability of the risk management practises and controls.

As there are many theories of economic crime, fraud and corruption, there are many different definitions as well. Despite the differences of the definitions, there are also similarities between those definitions. Below are stated some of the definitions as examples:

Finnish police has defined economic crime as follows: "A criminalised act or omission which is committed in the framework of, or using a corporation or other organisation. The act or omission is committed with the aim of attaining unlawful direct or indirect benefit. A criminalised, systematic act or omission that is similar to entrepreneurship and has the aim of considerable benefit is also defined as economic crime."

According to the International Standard on Auditing – ISA 240, the term fraud refers to "an intentional act by one or more individuals among management, those charged with governance, employees, or third parties, involving the use of deception to obtain an unjust or illegal advantage." Additionally in ISA 240 they have divided fraud into two categories, management and employee fraud; fraud involving one or more members of management or those charged with governance refers to "management fraud" and fraud involving only

employees of the entity refers to "employee fraud". Furthermore they remark the possibility of collusion within the members of the entity or with third parties outside the company. This is the chosen fraud definition, which is used throughout this study.

The Institute of Internal Auditors (2004) defines fraud as follows: "Any illegal acts characterized by deceit, concealment or violation of trust. These acts are not dependent upon the application of threat of violence or of physical force. Frauds are perpetrated by ***parties*** and organizations to obtain money, property or services; to avoid payment or loss of services; or to secure personal or business advantage.".

From the practitioners point of view the simple definition of fraud could be "any deliberate unethical act in business" according to the Samociuk and Iyer (2003). However, definitions are not universally the same, because same wordings might have diverse meanings in different cultures. For example what might terms unjust or illegal mean for persons coming from different cultures?

Another kind of a practitioner's definition is provided by the Association of Certified Fraud Examiners (henceforth ACFE) (2004). They concentrate on the "occupational fraud" and have defined the concept as "The use of one's occupation for personal enrichment through the deliberate misuse or misapplication of the employing organization's resources or assets." ACFE states all occupational fraud activity is clandestine, violates the perpetrator's fiduciary duties to the victim organization, is committed for the purpose of direct or indirect financial benefit to the perpetrator, and costs the employing organization assets, revenue, or reserves. However, occupational fraud is only a subcategory of fraud, although significant and perhaps the most investigated of all frauds.

In the KPMG Airline Fraud Survey (1995) the term fraud refers to "An intentional act, falsehood, omission or deceit, which results in a loss, or risk of loss, of any property, money or right.".

In a common language fraud refers to deceit, trickery or cheating according to the Webster's New World dictionary. As well, deception is stated to be the synonym for the fraud. Basically in a common usage fraud means lying, however, in legal terms there are additional elements needed to be proven in order to have a fraud claim.

In the Finnish criminal law (36:1) there is stated the following on fraud and other dishonesty:
“

(1) A person who, in order to obtain unlawful financial benefit for himself/herself or another or in order to harm another, deceives another or takes advantage of an error of another so as to have this person do something or refrain from doing something and in this way causes economic loss to the deceived person or to the person over whose benefits this person is able to dispose, shall be sentenced for fraud to a fine or to imprisonment for at most two years.

(2) A person who, with the intention referred to in (1), by entering, altering, destroying or deleting data or by otherwise interfering with the operation of a data system, falsifies the end result of data processing and in this way causes another person economic loss shall also be sentenced for fraud.

(3) An attempt is punishable.”

Furthermore to get a broader picture of the legal definitions from abroad, California Supreme Court defines fraud as a tort in the following way. According to it there are five different elements of fraud as a tort:

-Misrepresentation (false representation, concealment, or nondisclosure).
-Knowledge of falsity (or "scienter").
-Intent to defraud, that is, to induce reliance.
-Justifiable reliance.
-Resulting damage.

Each of these elements needs to be further analysed and in fact these five elements contain a number of components (see Engalla versus Permanente Medical Group, Inc. (1997) 15 Cal.4th 951, 964 Cal.Rptr.2d 843, following the definition in Lazar v. Superior Court (1996) 12 Cal.4th 631, 638,49 Cal.Rptr.2d 377.).

Differences between scholars and law definitions of fraud are in the comprehensiveness of the definitions and the rules how a crime is defined. Scholars tend to include injustices in the definition, however, it is very difficult to judge them in an equal way. Similarities include deliberate deceives and damages to another.

In a broad legal sense a fraud is the crime or offence of deliberately deceiving another in order to damage them, but the exact details vary among the jurisdictions. Because there is not any unanimous definition between scholars, politicians and law and practitioners for the economic crime or fraud, these concepts are taken and used in this paper in a broad sense.

Because this study is practically oriented, the term fraud refers here to the ISA 240 definition instead of legal definitions. The usage of ISA 240 definition of fraud is because of consistent and standardised identification, measurement and communication of various frauds.

2.3. Definitions, corruption

A very close term to the fraud is corruption, which could be seen describing the same unethical fraudulent acts in the macro level, while fraud could be seen merely happening in the micro level Samociuk and Iyer (2003). In a common language corruption refers closely to the extortion and bribery. In the Transparency International's (henceforth TI) Guidance document for the Business Principles for Countering Bribery TI has used a slightly amended definition of corruption from the UK's Law Commission draft Bill on Corruption in 2000 (Legislating the Criminal Code: Corruption, No. 248, March 1998). The amended definition states:

"The essential concept [of corruption] is that of influencing someone to act, in the belief that he or she will probably do so primarily in return for the conferring of an advantage (offering a bribe) on that person or a third party. Thus, a person who confers an advantage should be regarded as doing so corruptly if he or she intends a person, in performing his or her functions, to do an act or an omission, and he or she believes that if the person did so, it would probably be primarily in return for the conferring of the advantage.

Similarly, 'acting corruptly' is also accepting an advantage, believing that it was offered corruptly (accepting a bribe), or acting as the result of such an advantage (acting on a bribe). In every case, it is immaterial whether it is the person being bribed, or a third party, who receives the advantage. It is also immaterial whether or not the person accepting the bribe actually acts, or fails to act, as required; the accepting in itself is corrupt"

OECD defines corruption as "The abuse of public office for private gain." In this study it can be extended to apply also the abuse of private offices. This is the corruption definition used in this study.

In the Finnish Criminal law (30:7-8) (Business offences) there is stated as follows:
"Bribery in business
A person who promises, offers or gives an unlawful benefit (bribe) to
(1) a person in the service of a businessman,
(2) a member of the administrative board or board of directors, the managing director, auditor or receiver of a corporation or of a foundation engaged in business, or
(3) a person carrying out a duty on behalf of a business,
intended for the recipient or another, in order to have the bribed person, in his/her function or duties, favour the briber or another person, or to reward the bribed person for such favouring, shall be sentenced for bribery in business to a fine or to imprisonment for at most two years.

Acceptance of a bribe in business
(1) A person who
(1) in the service of a business,
(2) as a member of the administrative board or board of directors, the managing director, auditor or receiver of a corporation or of a foundation engaged in business or
(3) in carrying out a duty on behalf of a business
demands, accepts or receives a bribe for himself/herself or another or otherwise takes an initiative towards receiving such a bribe, for favouring or as a reward for such favouring, in his/her function or duties, the briber or another, shall be sentenced for acceptance of a bribe in business to a fine or to imprisonment for at most two years."

To be consistent in definitions, this study uses OECD definition for corruption. Use of this commonly accepted criterion for corruption helps in identification, measurement and communication of the results.

2.4. History of fraud and corruption

After the first introduction of the concept of "white-collar" crime in 1940 by Sutherland, it took two decades to wake the public and political interest on economic crimes in criminological discussion. In the end of 1960s and beginning of the 1970s the academic, popular and political interests aroused towards economic crimes. Especially criticism aroused towards corporate misconduct and politicians involved. There was a social and political moment to launch initiatives to control economic crime. However, established working committees investigating problems were only ad-hoc based and related to specific fields of economic crime.

On 1980s onwards there has been an international trend in developed industrial countries to decrease the control of economic crimes and increase the focus on control of ordinary crime according to Snider (2000). Even though working committees continued their work to control economic crimes, Snider argues (1993) that enforcement activities tends to focus upon the smallest and weakest individuals and organizations and any sanctions imposed are largely insignificant.

In the early 1990s academic research on economic crimes began to grow. 1990s criminal justice policy in North America and Western Europe drifted towards a law and order society, however such trends have not extended to economic crime according to Slapper and Tombs (1999). On the other hand, some forms of economic crimes have been in the particular interest of governments. For example, in Britain, certain forms of financial crimes, such as serious fraud, became the focus of critical state scrutiny according to Levi (1993) and Killick (1999). Nevertheless, these efforts could be understood in terms of their symbolic effects according to Fooks (1999). However, some states have tried to combat all forms of economic crime with new approaches. In 1995 United States Sentencing Commission hold its first corporate crime symposium. The purpose of the commission is to establish, assist and advice in crime and punishment policies and practices. From other countries Denmark had established a Contact Group on Economic Crime in 1997, Economic Crime Intelligence Unit in 2001 and the *"Danida Action Plan to Fight Corruption"* in 2003. Sweden established a discrete agency for combating economic crime, Swedish National Economic Crimes Bureau in 1 January, 1998. Norway followed in 2004 with its action plan for combating economic crime.

In Finland the trend has been opposite compared to other developed western countries. There has been a general shift in criminal justice policy and practice towards decreasing tolerance, widening criminalisation, and increasing punitiveness towards all types of illegal and anti-social behaviour, whether organised around so-called 'street' or economic crime according to Alvesalo (1998). Finland established its first action plan to reduce economic crime and the grey economy (Finnish Government, 1996) followed by two other governmental action programmes in 1999 and 2002. As well, in 2003 the government has shown interest towards Economic crime control according to Alvesalo (2004).

In a world scale, the 21st century started with the fear of terrorism. After September 11, 2001 terrorist attack to the twin towers in New York, USA, controls of terrorism have been tightened. Attitudes towards organized crime as well economic crime and money laundering have been tightened leading for example to the increased control of tax havens. In 2002 US introduced Sarbanes-Oxley act of 2002 after the huge corporate collapses, such as WorldCom, Enron and Arthur Andersen in order to save the credibility of the world biggest economy. This development has its effects also in Europe and in Finland in a form of new laws, regulations and recommendations, for example in the form of introduction of the corporate governance guidance. Politics, law enforcement agencies and non governmental organization interests have accelerated this development and brought more awareness of the fraudulent activity in the society. Awareness has brought more fraudulent incidents into public, thus increasing the importance of fraud risk management in order to prevent fraudulent activity.

2.5. Criminal motivation theories

For the deeper understanding of the causes of economic crime this paper introduces different theories of crime. Some scholars apply these general criminological theories to economic crimes as well, while other scholars have doubts about the suitability. At least categorisation of crime theories shed light to the possible reasoning of the causes of crime and economic crime as well. These kind of criminological theories have been used for example for political purposes and categorisation helps to understand the development of crime theories. Crime theories and categorisations are important in this paper, because they enlighten possible causes of crime. Even though theories listed here are not completely adequate models to explain all possible economic crime, fraud and corruption aspects, they can be used as a basis for further discussion. These discussions can be then used to develop measures to punish fraudsters, treat the effects of fraud or prevent possible frauds. In the table below are listed

theories of crime, their motives and causes from the Criminology Mega-Site, http://faculty.ncwc.edu/toconnor/criminology.htm, 17.12.2005.

Table 1. Motives and causes of crime

Table 1. presents theories of motives and causes of crime in chronological order from criminology and other fields.

Theory	Motive
Theology (1215 BC-present)	God's will
Education (1642-present)	Academic underachievement/bad teachers
Psychiatry (1795-present)	Mental illness
Psychoanalysis (1895-present)	Subconscious guilt/defense mechanisms
Classical School of Criminology (1690--)	Free will/reason/hedonism
Positive School of Criminology (1840--)	Determinism/beyond control of individual
Cartography (1800-present)	Geographic location/climate
Imitation (1843-1905)	Mind on mind crowd influences
Economics (1818-present)	Poverty/economic need/consumerism
Case Study Approach (1909-present)	Emotional/social development
Social Work (1903-present)	Community/individual relations
Sociology (1908-present)	Social/environmental factors
Ecology (1927-present)	Relation of person with environment
Differential Association (1939-present)	Learning from bad companions
Anomie (1938-present)	State of normlessness/goal-means gap
Differential Opportunity (1961-present)	Absence of legitimate opportunities
Alienation (1938-1975)	Frustration/feeling cut off from others
Identification (1950-1955)	Making heroes out of legendary criminals
Containment (1961-1971)	Outer temptation/inner resistance balance
Prisonization (1940-1970)	Customs and folkways of prison culture
Gang Formation (1927-present)	Need for acceptance, status, belonging
Behavior Modification (1938-1959)	Reward/Punishment Programming
Social Defense (1947-1971)	Soft targets/absence of crime prevention
Guided Group Interaction (1958-1971)	Absence of self-responsibility/discussion
Dysfunctional Families (1958-present)	Members "feed off" other's neurosis
White-collar Crime (1945-present)	Cutting corners/bordering on illegal
Control Theory (1961-present)	Weak social bonds/natural predispositions
Strain Theory (1954-present)	Anger, relative deprivation, inequality
Subcultures (1955-present)	Criminal values as normal within group
Labeling Theory (1963-1976)	Self-fulfilling prophecies/name-calling
Learning Disabilities (1952-1984)	School failure/relying on "crutch"
Nutrition and Diet (1979-present)	Imbalances in mineral/vitamin content
Metabolism (1950-1970)	Imbalance in metabolic system
Biofeedback (1974-1981)	Involuntary reactions to stress
Biosocial Criminology (1977-1989)	Environment triggers inherited "markers"
The "New Criminology" (1973-1983)	Ruling class oppression
Conflict Criminology (1969-present)	Structural barriers to class interests
Critical Criminology (1973-present)	Segmented group formations
Radical Criminology (1976-present)	Inarticulation of theory/praxis
Left Realism (1984-present)	Working class prey on one another
Criminal Personality (1976-1980)	53 errors in thinking
Criminal Pathways Theory (1979-present)	Critical turning/tipping points in life events
Feminism (1980-present)	Patriarchial power structures
Low Self Control Theory (1993-present)	Impulsiveness, Sensation-seeking
General Strain Theory (1994-present)	Stress, Hassles, Interpersonal Relations

Source: The Criminology Mega-Site, http://faculty.ncwc.edu/toconnor/criminology.htm, 17.12.2005.
This table shows the variety of theories trying to explain different types of crime. However, none of these theories is fully adequate to explain all types of crime.

2.6. Fraud risk management

Fraud risk is the biggest unmanaged sole risk in a company according to the Samociuk, Iyer and Lehtosuo (2004). However, there are many ways to manage risks, including fraud risks. This section describes the risk management process.

According to Jorion (2000), risk management process can be divided into four phases. The process starts with the formulation of the strategy. It is recommendable to apply enterprise wide risk management strategy, because it takes into account all the risks what a company might face. Fraud prevention strategy is thus part of the enterprise wide risk management strategy and has to be in line with the goals of the company.

After the strategy has been defined, second phase of the process starts with the identification of the risks. Categorisation of the risks can help the identification process. There are several ways to categorise different fraud risks, where one is the categorisation of the ACFE (2004).

Third part of the risk management process is risk assessment. Risk managers can use stress testing, which can rely on scenario analysis. It is known that objective probabilities are a bad estimate of true probabilities. However, it is the work of the risk managers to provide assessments of the probabilities as objective as possible. In fraud risk assessment, historical events can be used as guidance for estimation of events, their severity and probabilities. Fraud risks are, however, very complex and rapidly evolving with the technology and thus prospective scenario analysis could provide significant benefits to the risk assessment.

Fraud risk assessment differs from other risk assessments in one important sense, it is about people. Fraud is happening only due to human behaviour as opposed to the other risks, which can happen due to many reasons not necessarily relating to people at all. Human behaviour is one of the reasons for the complexity of the fraud risk.

Fourth part of the risk management process is control. Assessed risks need to be controlled somehow. There are four options that risk managers can make according to Comer (1998),

they can try to avoid, reduce, transfer or accept risks. Control methods should be balanced to with the costs they are causing to the business. Additional, unnecessary controls do not create value, but slows down business processes. As well, control methods should be balanced according to the benefits from avoiding possible risks. Some control methods might be too costly for minor and low impact risks; therefore acceptance of risks is justified from cost/benefit perspective.

Risk management process: (Jorion, 2000)

1. Strategy.
2. Identification.
3. Assessment.
4. Control.

Samociuk and Iyer (2003) have presented a fraud management strategy for all companies, it is based on the following six components:

1. Define objectives.
2. Understand the risk.
3. Reduce the risk.
4. Detect attempts.
5. Manage incidents.
6. Review & enhance.

Identification of the fraud risks can be based to previous incidents, lists of commonly known schemes or scenario analysis. As frauds are complex and schemes are developing rapidly with the technology, identification of the threats becomes important. Identification can be proactive or reactive.

Assessment of a certain fraud risk can be done based on the probability of a certain fraudulent scheme and multiplying it with the estimated losses attributed to that scheme. Estimated recovery of the losses can be taken into account as well. Below is a formula for a certain fraud risk assessment.

$$E[risk] = P(scheme) \times E(losses) - E(recovery),$$

where E(risk) is the estimated risk, P(scheme) is the probability of a certain fraudulent scheme, E(losses) is the estimated losses attributed to certain fraudulent scheme and

E(recovery) is the estimated amount of recovery from the certain fraudulent scheme. As fraud schemes are developing rapidly, there is not always historical data available where to base the estimates. Then expert opinion can be used as risk assessment.

According to Comer (1998), risks can be categorized into four groups based on the probability and criticality of the schemes. Probability can be either high or low as well as criticality can either cause high or low costs. Comer suggests different measures for the categorized fraud schemes as stated below in the figure 1. Measures include avoidance, reduction, transfer and acceptance of fraud risks.

Figure 1. Fraud categorization based on probability and criticality and measures for categories.

Probability/ Criticality	Frequent	Infrequent
High cost	Category 1 Risk avoidance Risk transfer Risk reduction	Category 2 Risk transfer Risk reduction
Low cost	Category 3 Risk reduction	Category 4 Risk acceptance Risk reduction

Source: Comer, M. p. 469 (1998)

Comer suggests that in category 1, where the probability of the fraud is frequent and criticality is high, the controlling measures includes risk avoidance, transfer and reduction as the significance of this category is the biggest for the company. In category 2, where the probability of the fraud is infrequent and criticality is high, controlling measures include risk transfer and reduction. As the frauds in this category are happening infrequently, the total avoidance of these incidents can become costly. In category 3, where the probability of the fraud is frequent and criticality is low, controlling measure include only risk reduction. As the impact of fraud is low, it can become too costly for companies to transfer or avoid the risk. In category 4, where the probability of the fraud is infrequent and criticality is low, controlling measure includes as well risk reduction, but also risk acceptance. The category 4 is the most insignificant for the company. Comer suggests risk reduction for all of the fraud categories.

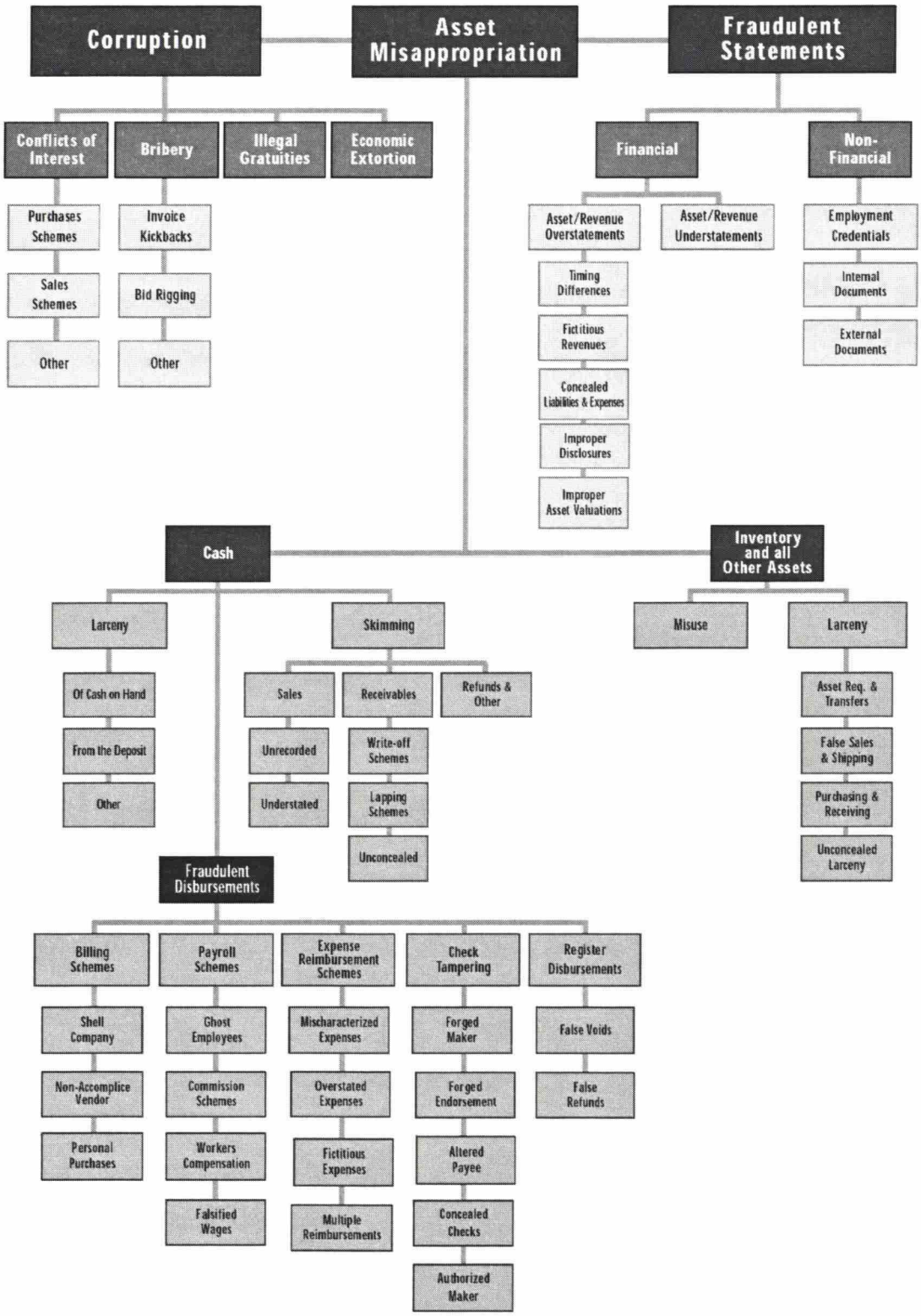
2.7. Fraud categorisation

Fraud categorization can be done on the basis of characteristics of the fraud cases. There are other categorisations in addition to the Comer's fraud categorisation presented in section 2.6. Fraud risk management. The examples of separation criteria can be based on the following six characteristics:

-Concealment, conversion
-Concealed, unconcealed
-Duration: one-time smash & grab, repeating systematic frauds
-Internal, external, collusion
-Criticality: high cost, low cost
-Probability: frequent, infrequent

In the ACFE (2002) classification system (Figure 2.) occupational fraud is divided into three main categories, corruption, asset misappropriation and fraudulent statements. This system follows the frequency of different fraud schemes. ACFE found out that in this categorisation over 85 % of occupational fraud cases fall in the asset misappropriations category. Asset misappropriations are then divided into two subcategories, cash and inventory & all other assets. Results indicate that over 90 % of asset misappropriation schemes fall into the cash subcategory. Cash subcategory is then separated into three different groups, larceny, fraudulent disbursement and skimming. Following the same procedure, over 70 % of cash schemes belong to the fraudulent disbursement group. Finally, most of the fraudulent disbursements fall into 5 different subgroups, billing schemes, payroll schemes, expense reimbursement schemes, check tampering and register disbursement schemes. From these subgroups, fraudulent billings are most common with over 45 % frequency and check tampering follows with over 30 % frequency. Figure 2 represents the classification of occupational fraud and abuse in the ACFE (2002) study.

Figure 2. Occupational fraud and abuse classification system.



Source: ACFE (2002).

ACFE has made a similar survey on 1996 and those comparable results point out that the order of grouping has not changed. Also there have not been major changes in the frequencies during these studies.

In KPMG fraud survey 2003, the classification is general, but they haven't reported the definition used in that survey. Figure 3. shows the seven fraud categories used in the survey.

Figure 3. Fraud categories assessed in KPMG survey.

Misconduct -Conflicts of interest -Insider trading	**Medical/Insurance Fraud** -Medical/insurance claims fraud -Policy churning -Workers' compensation fraud
Consumer Fraud -ATM theft -Check fraud -Credit card fraud -Fraudulent classification of merchandise for customers -Fraudulent merchandise returns -Identity theft	**Vendor-Related and Other Third-Party Fraud** -Bid rigging and price fixing -Bribery -Diversion of sales -Duplicate billings -Extortion -False invoices and phantom vendors -Inventory theft -Kickbacks and conflicts of interest -Loan fraud -Theft of intellectual property
Employee Fraud -Check fraud -Expense account abuse -Payroll fraud -Pension theft -Theft or misappropriation of assets	**Financial Reporting Fraud** -Asset revenue misstatement -Concealed liabilities and expenses -Improper revenue recognition -Inadequate omissions or inappropriate disclosures
Computer Crime -Hacking and other cyber-theft	

Source: KPMG (2003).

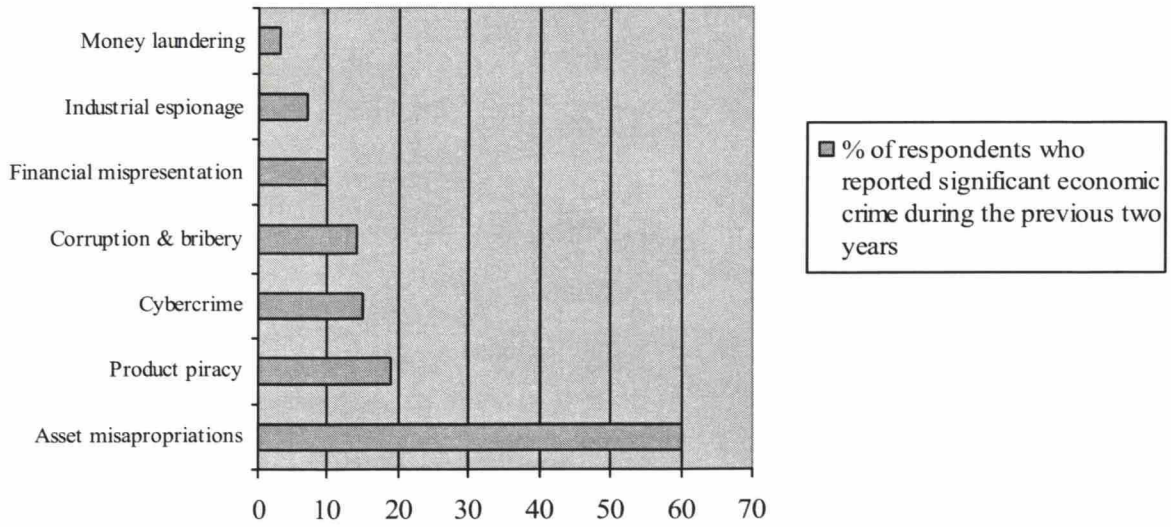
In KPMG classification (2003) frauds are divided into 7 broad categories, which are computer crime, consumer fraud, employee fraud, financial reporting fraud, medical/insurance fraud, misconduct and vendor related and other third-party fraud. According to this survey, 60 % of organizations experienced employee fraud during the prior 12 months, indicating that employees are the biggest source of fraud. Second largest category is consumer fraud with 32 % occurrence rate. This employee fraud category includes check frauds, abuse of expense account, payroll fraud, pension theft, theft or misappropriation of assets. The results are difficult to compare to the ACFE survey, because of the different categorisation. However, there are still some similarities to other studies such as to Ernst & Young (E&Y) (2003) survey, which states that some 85 % of the worst frauds are committed by insiders.

The official statistics includes only those fraud cases, which are reported to the government regulatory agency or law enforcement, thus leaving a large number of cases uncovered. According to KPMG's fraud survey 2003, 64 % of the companies reported their fraud incidents to officials.

Some classifications are not based on victimisation studies thus offering a different point of view. The classification represented by Howard Davia (2000) divides the fraud cases into three sectors: Sector 1 includes all the fraud that has been or is being prosecuted, which is estimated to cover 20 % of all fraud cases. Sector 2 includes all the fraud that victims have discovered, but which has not prosecuted. This sector is estimated to cover 40 % of all fraud cases. Finally sector 3 includes all the fraud that has not been discovered. This sector is estimated to cover the rest 40 % of all fraud cases. This classification covers all types of frauds, but focuses only on prosecuting.

In the PricewaterhouseCoopers' (PwC) Economic Crime Survey (2003) the term fraud and economic crime is converged and is defined as "The intentional use of deceit to deprive another of money, property or a legal right." They have categorized frauds in a broad scale as can be seen from the figure 4.

Figure 4. Fraud categorisation by PwC.



Source: PwC (2003).

PwC divides the type of frauds experienced into 7 categories (money laundering, industrial espionage, financial misrepresentation, corruption & bribery, cyber crime, product piracy and asset misappropriations), where asset misappropriations seem to be most prevalent fraud type. 37 % percent of respondents worldwide experienced significant economic crime during the past 2 years and from those 60 % experienced asset misappropriations.

In E&Y study (2000) the definition of fraud has not been published, but it is said that it "involves deceit and concealment". In this study they do not represent a categorization by fraud types.

2.8. Laws and regulations

Openness seems to be the best protection against frauds, because the possibilities to conceal fraudulent activities are then much harder. Big corporate scandals and media coverage has amplified the importance of openness and proper corporate governance. Therefore governments, regulators, and shareholders together with sharpening public opinion are putting intensifying pressure to the corporate governance issues. In general, laws and regulations regarding fraud are a consequence of big frauds, which have received wide media coverage. A good example is Sarbanes-Oxley Act of 2002 after Enron disaster.

There are several guidelines and frameworks focusing to the corporate governance and internal controls, such as Corporate Governance Recommendations for Listed Companies

(2003), the Executive Summary of the King Report from the Institute of Directors in Southern Africa (2002), the Ramsay Report (2001), the Turnbull Report (1999) and the Committee of Sponsoring Organisations of the Treadway Commission's (henceforth COSO) Internal Control – Integrated Framework report (1992). Even though all regulations are not mandatory, they put certain pressure on management to manage fraud. Regulations put into action help frauds to get discovered and thus increases information about frauds. Additional information and awareness improves fraud and corruption detection, reporting and measurement, which in turn can be used to develop better fraud and corruption management tools.

In the banking sector, the Basel Committee on Banking Supervision has put more pressure to control operational risk under the new Capital Accord (Basel II), due to come fully into effect by year-end 2006. Banks need to hold capital to protect against operational risk losses; however, banks may use their own method assessing their risk to operational risk. The more sophisticated risk management systems allow less capital allocation for operational risks compared to the basic and standardised approaches.

In the wider scale, the regulators and legislators are also seeking improvements in the reporting framework by adopting new laws. In the US for example, President Bush signed Sarbanes-Oxley Act of 2002 into a law in August 2002. The purpose of the act is to protect investors by improving the accuracy and reliability of corporate disclosures. The law requires that executive officers and chief financial officers must implement internal controls and certify that all frauds have been reported to the auditors and audit committee. It applies also to those who have significant roles in controls. The new European company law directive seems to strengthen shareholder rights and third party protection due to proposals to the corporate governance guidance according to the Commission of The European Communities' Action plan (2003). However, the plan recommendations imply that the objectives of combating fraud and abuse of companies should be achieved through specific law enforcement instruments outside company law. For example in Finland this means the use of Crime law. One example of combating against fraud and corruption is the right of the general prosecutor to file a law suit against companies for example in case of bribery.

3. Fraud cost

Economic crimes cost about 4 % of Britain's gross domestic product or £40 billion according to accounting and consultancy organisation RSM Robson Rhodes LLP (2004) and they say it could be just the tip of the iceberg. ACFE anti-fraud specialists estimate that the typical U.S. organization loses 6 % of its annual revenues to fraud. If it is applied to the US gross domestic product for 2003, it translates to $660 billion in annual fraud losses. In Finland Jokinen, Häyrynen, and Alvesalo (2002) estimate economic crime amounting to € 0,7 – 1,7 billion annually. That is approximately 5 % of Finnish gross domestic product in 2002. According to these estimates fraud and corruption costs are substantial and worldwide phenomena.

The number of reported fraud cases is increasing. According to the KPMG's Fraud Survey (2003), the experienced number of a broad range of frauds in the US organizations during the prior 12 months has increased from 62 % to 75 % in the period from 1998 to 2003 – an increase of 13 percentage points in 5 years. In the PricewaterhouseCoopers (PwC) (2003) survey, the number of serious frauds during the previous two years in the Western Europe has grown from 29 % in 2001 to 34 % in 2003 – a 5 % percentage point increase in two years. In Central and Eastern Europe the same figures are 26 % and 37 % representing an increase of 11 percentage points. In the Ernst & Young survey (2003) they have looked the number of headlines related to fraud reported by Reuters business briefing over time. In 10 years the average annual number of headlines seems to have more than doubled to nearly 90 000. This shows that media coverage has increased and thus it contributes to public opinion and reactions.

There seem to be two basic reasons behind this development, firstly the level of awareness of fraud has increased and secondly the demands for openness and transparency have increased leading to larger detection rate. The growing number of frauds reported has opened the eyes of managers to look closer their activities. Additionally to the increased detection rate, it is also possible that frauds are becoming more common, because of the eroding business ethics.

The discussion has been going on what should be included in fraud costs and how these costs should be measured. There's a gap between crime discussion, legal definitions and practitioners. In this gap there is a huge grey area, where actions are not necessary going in

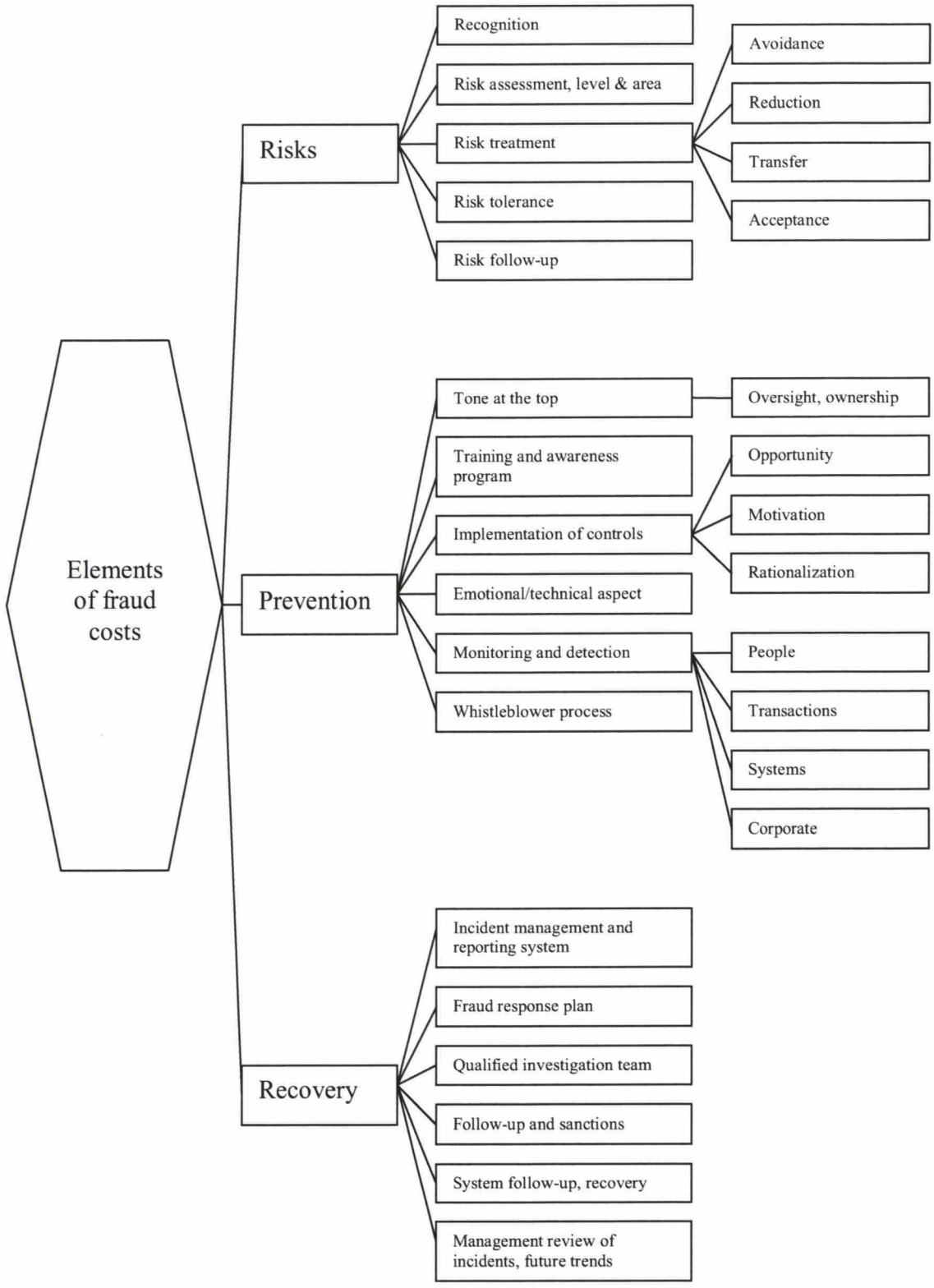
line with good social conduct or business norms. Whether those actions are right or wrong depends on the situation. Thus quantifying fraud costs is difficult. There are several problems related to this subject. First of all, fraud costs are hidden in their nature. This means that most of the frauds are never revealed. Howard Davia estimates in his book "Fraud 101" that 40 % of frauds are not discovered. He estimates also that 40 % of frauds are known only by few, but they are not made public or prosecuted. Secondly, there are no generally used criteria to identify fraud, corruption or economic crime. Therefore fraudulent incidents are not always observed, neither reported. Even though there are some official statistics about economic crime, they are flawed because of the reasons explained above. Thus official statistics do not show fraud and corruption costs to companies. Thirdly, a large part of the total fraud costs are estimated to be indirect costs. They are very difficult to measure as they are usually intangibles, such as reputation, image and customer relationships.

In this study fraud costs are divided into three different types based on the time of occurrence of the costs. The basis for total fraud costs is in risk of fraud, the potential fraudulent incident facing the company. These risks are leading to potential costs. Risks form the first cost element in this study. As the companies aim to manage all or part of these risks, it requires efforts from them. These preparations and efforts outline the second cost element for companies, namely prevention costs. Finally, if the fraudulent incident happens regardless of the preventive measures, it is causing damages to the company. However, companies can recover fully or partly from the damage fraudulent incident has caused them. Recovery is not actually a cost, but is essential part of the total fraud cost measurement. Thus the last cost element relates to the recovery from damages. These elements form the total cost of fraud, T, which is calculated as

$$T = R + P - D,$$

where R is the potential cost arising from the fraud risk, P is the risk prevention cost and D is the recovery from the fraud damages. This formula can be used to calculate total fraud costs on a given period of time. The following figure 5. summarizes the elements of fraud costs. Each of these elements is discussed further in the following sections.

Figure 5. Elements of fraud cost.



3.1. Fraud risk

The first cost element in this study is fraud risk, which is causing potential costs to the company. Risk is defined in the Institute of Internal Auditors (2007) as "The possibility of an event occurring that will have an impact on the achievement of objectives. Risk is measured in terms of impact and likelihood." The likelihood of a fraud depends on the probabilities of the threat and vulnerabilities. The impact of a fraud risk can vary significantly, but it is estimated that a typical company loses 6 % of its annual revenues to fraud according to ACFE (2004). According to the Samociuk, Iyer and Lehtosuo (2004), fraud risk is the biggest unmanaged sole risk in a company. The assessment of the fraud risk depends on the risk recognition and identification. If the fraud risk is not managed properly in the companies, there exists vulnerabilities and thus the likelihood of fraud is higher than properly managed companies. Fraud risk can affect significantly to company value, which is best seen in the bankruptcy of Enron Corporation. However, fraud risks can be avoided, reduced, transferred or accepted according to Comer (1998). The used method depends on the company's risk tolerance.

To measure the total fraud risk, it can be divided into different classes. One way to classify fraud risks is based on the object of the fraud. They can be personnel, information, material or business operations related. Probabilities of individual classes of events and the corresponding impacts are then estimated either quantitatively or qualitatively. Estimation of the impacts could be challenging as fraud impacts can be direct or indirect, tangible or intangible or one time or continuous. Risk of an individual class is the product of the probability and the related impact. The total fraud risk is the sum of the risk in individual classes. As the fraud risks are person related and developing rapidly with the technology, the risk follow-up is important to correct assessment. Thus fraud risk profiles should be updated regularly.

When total fraud costs are calculated from a period of time, which has already passed, realized risks are known and they are then historical fraud costs. There is no uncertainty related to the known incidents, thus the total fraud costs can be calculated easier from the past. These past fraud cost calculations can be used as an estimate for the future fraud costs.

3.2. Fraud prevention costs

Second cost element is prevention costs. They arise either before the fraud incident has happened due to the preventive methods or after the fraud incident when preventive methods

need to be reviewed and improved. Prevention costs include all the proactive measures company is taking in order to manage and reduce fraud incidents, for example employee fraud prevention training. The measures used depend on the tone at the top and thus on the ownership of the processes. Company executives have a great responsibility on deciding the prevention level in the company. Prevention costs can be a mixture of fixed and variable costs depending on the preventive methods used. There are three main things companies need to do in order to prevent frauds according to Albrecht and Wernz (1993).

-reduce the opportunity to commit fraud and increase the probability of getting caught.
-reduce motivation to commit fraud.
-reduce ways to rationalise the act of fraud.

In order to reduce the opportunity to commit fraud and increase the probability to get caught companies can implement controls. They are based on risk assessment, balanced both to protect honest personnel and prevent and detect dishonest practises. Controls can have various types, such as intelligence, preventive, reactive, reconstructive or monitoring and enforcement according to Comer (1998). He also specifies that controls can be hardware, specific policies and procedures, technical controls or organisational controls. There is a trade-off between controls and flexibility of the business operations. However, some of the controls do not affect negatively to the flexibility of business operations. Prevention costs arise mainly from various methods of controls. However, some of the control costs can be shared among other risks and they are not only attributable to fraud risk.

There are several ways of controls, for example separation of duties, authorisation of transactions, access controls, records, standards, guidelines, monitoring of red flags, periodic internal and external audits and risk profiling. The list is not complete, but gives an idea of the possibilities. Typically monitoring actions and controls can be divided into different levels, for example to people, transactions, systems and the whole corporate level controls.

The second way of prevention relates to the fraudster's motivation to commit a fraud. Company can use emotional controls to reduce the motivation for example through good working conditions and benefits from the achievements. One part of the good working condition is to respect employees, for example through providing necessary support for those who might have personal problems. Motivation to commit fraud can be reduced by increasing

the knowledge of the risk to get caught. This can be done by informing employees about the monitoring and making the detections known. Detections can be made known for example as case examples in the fraud prevention training. Additionally, anonymous reporting or whistleblowing is also an effective way to increase the knowledge of the risk to get caught as anyone can report suspicious actions without fear of revenging consequences. Emotional aspect is preventing methods is relatively large as fraud risks are solely people related risks.

Third preventive method relates to the reduction of the fraudster's rationalization of the act of fraud. Employee may rationalize the justification of fraud if they see others doing fraud. For example a store owner taking a bag of toilet papers without paying at that time can be seen as manager using company belongings to her personal use. Employee might think it is justified to steal if the managers are doing it as well. Therefore by showing good example and emphasising the corporate culture which does not tolerate any kind of fraud company can reduce the rationalization of the act of fraud. Other ways are for example the use of company's ethical principles and well communicated internal and external guidelines and policies against fraud. Employee training can be used for this purpose as well. Also punitive reactions to act of fraud, like dismissal and prosecution of fraudsters, enhances the good corporate culture. As well, reporting of all criminal acts to the police are reducing the rationalization of the act of fraud as company clearly states that it is not tolerating any kind of fraud.

The other cost besides of the proactive measures is the cost from the improvements of the prevention methods. Monitoring measures can detect a fraud incident for example through the whistleblower process, where employees report their suspicions to the risk management. After the incident companies typically review and improve their controls in different levels in order to prevent further incidents happening. These improvement costs may become in some fraud cases even larger than the actual direct losses from fraud. Prevention and improvement costs are usually known better than the risks. They can be calculated using the expenses from the controls or estimated by using the budgeted expenses of the controls.

3.3. Recovery

Third cost element is recovery. It is not a cost, but it is an essential part of the total fraud cost measurement. Recovery from the damages from fraudulent activity can be partial, full or in extreme case the net effect from fraud could be even positive. The net effect can be positive

for example when the company has overinsured itself and thus benefits from the fraudulent event. Recovery from the fraud can come from different things which were damaged or lost, for example they can come in a form of positive reputation from quick resolution and good communication. Recovery from the incident depends on many things, for example the preparedness of the company to the incident, the corrective actions taken and the pace of investigations. This depends on the company incident management and reporting system. The faster information flows to the correct persons, the faster company can start preventive methods, which in turn can restrict the damages. Ready made fraud response plan helps achieving the fast and sufficient response to the fraud incident. Qualified investigation team knows how to act during the investigation, get the sufficient evidences and not let the fraudster to destroy them. Evidences help to bring the fraud case to court and to prosecution, where fraudsters can be punished and damages recovered. Additionally to these measures companies can prepare for the fraudulent incidents by outsourcing the risk to third party or taking insurance. Usually after a fraud incident management reviews the case and prepares improvement plans for the future to prevent further incidents.

Recovery can be calculated using the estimate of the damages and the recovery rate. Recovery is the product of those two. Recovery rate, r, is the rate of received benefits to damages. As recovery can be notes as the product of recovery rate and Risk, $D = r \times R$. Substituting this in place of the D in the total fraud cost formula, it can be written as $T = (1 - r)R + P$.

3.4. Comparison of fraud cost elements

Fraud risk, recovery rate and prevention costs form the total cost of fraud. Risk and recovery are naturally linked together, without risk there is no recovery. Risk is measured in terms of impact and likelihood and the likelihood of a fraud depends on the probabilities of the threat and vulnerabilities. The purpose of the preventive methods is to avoid or reduce company's vulnerabilities to fraud. Therefore preventive methods have a negative effect to probability of vulnerabilities and therefore a negative effect to risk. If any fraud risk is realized or the risk grows, it has consequences to the preventive methods as company typically aims to cover the loopholes of the controls or prepare for the risk. Thus increase in the risk of fraud increases the prevention costs in the long run. On the other hand reduced risk can justify decrease of the controls as unnecessary cost item. In the long run companies aim to be cost efficient. This means that risk and prevention are interlinked so that risk has a positive impact to prevention

costs and prevention has a negative impact to the risk. There is a continuous race between risk and prevention.

4. Methodology, Data and Analysis

4.1. Methodology

In this study I use face-to-face interviews to obtain detailed information, explanations and opinions about elements included when considering the cost of fraud and corruption. Interviews used in this study are conversational and semi-structured in their nature. Interviews are guided by questions, which had been delivered beforehand to the interviewees. Nevertheless, interviewees don't need to follow strictly the sequence of the questions, if they want to elaborate one or more of their explanations. However, all of the topics included in the questions are covered in the interview. Interview questions can be found in the appendix.

Interviews are not recorded, but notes are taken, which allows data analysis to be conducted later. This should help interviewees to feel more open about things. However, notes can be distorted as some information can be omitted from the answers. The intention was to keep this issue minimized. There are 29 open questions, which are divided into four segments: first of all general questions and then questions concerning fraud and corruption prevention methods, risks and incident management. The duration of the interviews varied from one to two hours. Interviews were taking place in the interviewee's company premises.

This method is chosen because the topic of fraud and corruption is controversial and there are different ways to define and see things, thus a brief conversation is needed to obtain better reliability of the answers. As the questionnaire was sent beforehand to the interviewees, they had the possibility to prepare for the questions, which could increase the accuracy of the answers in this case. The aim is not to make a survey for statistical purposes, because the topic itself is such that survey results can be easily challenged. Interviews enable a more detailed and in-depth approach to the problems than surveys. As well, the correct understanding of the questions can be checked immediately during the interview. This helps to overcome the poor recall bias.

Weakness of this method is that it is very time consuming, thus the number of interviews is limited. As well, interviews are subject to problems of bias due to response bias, inaccuracy

and poor recall. However, conversational method helps to overcome these problems. The study is qualitative and conversational, therefore results are merely guiding than statistically significant.

4.2. Data and analysis

Data for this study is acquired from five face to face interviews of the security, risk management and internal audit experts. These people have the largest responsibility to control risks and thus they are the subject matter experts. All of the interviews were conducted in Finland based companies or governmental agencies. These companies were selected by using the contacts from Hibis Scandinavia AS and Tuokko Tilintarkastus Oy. As the topic is sensitive in its nature it was regarded practical to use existing contacts. Using the existing contacts can cause a selection bias to the results. The selection of the companies and governmental agencies form a wide range of sound, large businesses, which have completely different business models.

In the questionnaire, there are 29 open questions divided into fours subgroups. Purpose of the first group of the questions, general questions, is to lead to the subject and verify the understanding of the terms and subject. Second group of questions dives into the topic relating to the prevention. Third group of questions is focused onto the risks and the last groups of questions concentrates onto the managing incidents and follow up. Answers of the interviewees have been compiled under each question and they are in the quotation marks.

Analysis of the answers and findings of this study are reported under the interview questions to help the readability. Analysis is prepared from each question. As some of the questions are answered together with another question, the analysis can contain information also from the other answers. As different kind of companies were interviewed, the results are divided into two sub groups, to government agencies and to listed companies. Two of the companies belong to the government agencies group and three other companies form the listed companies group. The results of these two subgroups are compared and analysed.

Findings are divided into groups based on the theme followed in this study. First set of fraud related costs rises from the fraud risk, causing potential costs to the companies. Before actual fraud has happened, companies prepare for the incidents and place efforts to avoid fraud

incidents and decrease the risk of fraud. Naturally this preventive methods cause costs. If risks are realized and actual fraud incident happens, it causes damages to the company. Companies can, however, recover from these damages.

This interview report is made based on the interviews conducted during 2006 from five different entities and six interviewees. Two of the entities are government agencies and three of the entities are listed companies. Interviews were conducted in government agencies on 9 June 2006 and 3 August 2006. Interviews in listed companies were conducted in 15 June 2006, 5 September 2006 and 16 November 2006. Due to the profiling issues of the answers and respect of the confidentiality of the entities, the names of the companies or entities are not published.

For simplicity, "company" refers here to the companies and governmental agencies. Word "fraud" refers here to fraud and corruption. The answers of the interviewees are presented below each question in quotation marks. All of the interviewees did not answer to all of the questions, thus some questions have less than five different answers. The answers below do not follow the same order of the companies from question to question.

Interview questions, answers and analysis

General questions

1.1. How do you define fraud?

"Fraud is defined in the crime law. There is an internal guidance on the topic, such as ethical principles, compliance guidelines and moral guidance. Fraud definitions could vary from one country to another."

"There isn't any clear definition for fraud. However, fraud could be criminal activity such as theft of cash, or a con or other activity against the guidelines, which is done purposely. "

"There isn't a precise definition for fraud. However, we are aware of EU and ISA fraud definitions. Fraud is intentional, planned and fraudsters are benefiting from it. At the same

time fraud can cause monetary losses but as well other kind of losses or damages, such as losing of reputation and customers. "

"Frauds are divided into two groups, to customer or vendor related and to personnel related. Frauds are related to money or other benefits and they are done purposely."

"We're managing frauds from broader point of view. We have recognised and prepared for over 30 models of fraud. We have defined frauds on the basis of the lines of businesses as the threats are in different scale."

Interviewees stated that fraud can be criminal activity, which is intentional and planned. They mentioned that frauds are done because fraudsters want to either benefit from it or cause damages. Fraudsters can be either insiders or from outside of the company, such as customers or vendors.

Interviewees recognized that losses from fraud can be direct, such as monetary losses or indirect, such as lose of reputation or customers. Interviewees referred to different fraud definition sources, such as crime law, ISA and EU definitions or their internal guidelines. Some of the interviewees noticed that there is not any common definition for fraud. Definitions can vary inside the businesses or from country to country according to the interviewees. The differences between the two subgroups were not clear as the answers deviated from interviewee to interviewee.

1.2. How important you regard fraud risk?

"Fraud risk is regarded as a significant risk, as all the incidents or attempts cannot be detected. Company is prepared for the risks."

"Fraud risk is regarded as a significant risk. Internationalisation increases the risk as the culture, regulations and knowledge is different in different countries."

"As a very significant risk. It is one of the main areas of concentration. Fraud risk is reported to the board to give true and fair view. Trust of our customers and financiers is at stake when fraud is considered."

"There is only couple of fraud incidents per year. In a monetary level frauds are not a significant issue; it's merely an ethical issue. Biggest issues are related to the information security and to stakeholders. Most fraud cases are related to same few persons. Roughly 90 % of total fraud costs are coming through building of controls and information systems. A bit more than 5 % is coming through actual fraud costs and less than 5 % is based on the fraud risks."

"Financially frauds are not significant threat for us. We're more concerned about our reputation as the effects of a small fraud incident could start growing and thus damage severely our reputation. For example there have been a case where one of our stakeholders acted fraudulently and press immediately connected us to unfair business, which damaged our reputation. We have documented the process from our side and reported it to authorities. Damages to the reputation affects negatively to our share price. Our reputational risk grows when business moves towards the east. However, the risk is not significant. Vandalism and damaging of our property do not pose a significant financial risk to us. It's inconvenient to us, but financial losses are rather small. I'd estimate that the biggest fraud related expenses arises from the risks. Controls are causing the second largest expenses and third largest expenses arise from prevention of the frauds."

Fraud risk is regarded as a significant risk in most of the companies. Reputation is mentioned to be the most significant risk. There are no differences between the governmental agencies and listed companies groups. Most of the interviewees stated that fraud costs are related merely to non-monetary, soft items, such as reputation, image or trust of customers. Companies are not only considering themselves when managing fraud, but also their stakeholders, such as suppliers, partners and customers.

Fraud risk is considered significant, one of the major risks to concentrate on. The amount and size of frauds varies among the companies and businesses. Controls, risks and realized risks are mentioned as the biggest fraud costs. Interviewees stated that not all incidents or attempts can be revealed as everything cannot be controlled. One interviewee stated that a small reputational risk in one area can grow into big measures due to mass media, which can then affect the whole business.

All companies doing business internationally stated that fraud risk grows when operating outside Finland. Attention is needed to manage international fraud risk, as regulations, culture and business environment is different in other countries according to one interviewee.

Prevention

Tone at the top

2.1. Who is responsible for managing fraud in your company?

"Executive management is responsible of the fraud risk management. Responsibility is then divided to the operational risk management and to the security department."

"Security is responsible for managing fraud risk. Line management and organisation is also responsible for the risk management. In a group level the owner of the process is responsible of the risks. Risk management department acts as a supporting department in an enterprise wide level."

"According the rules all employees are responsible for managing fraud. At the operative level, the owner of the activity or a project is responsible for it. Suspicions of fraud are reported to the managers. Finance and legal department are responsible in an enterprise wide level. However, in the end of the day, CEO has the responsibility at the highest level. "

"Board and CEO have the responsibility for managing fraud at the top level. Line managers are responsible for their own line of business. Centrally there are risk management support groups, which act as consultants and help business units to manage their risks. Internal audit works closely with risk management. Risk management is taken part of the measurement of internal units' results."

"The line management is responsible of the fraud management. We have enterprise wide support functions for fraud management, like corporate security and internal audit teams."

At the end of the day, executive management is responsible for managing fraud risk in most of the companies. Responsibility and ownership of the fraud risk management depends on the level of business in some companies. At a group level, owner of the process is responsible of managing fraud. In day to day business, responsibility is basically given to operative

management. One interviewee stated that all employees are responsible for managing fraud risk.

In many companies board of directors reviews risk management reports. However, only broad level risks are reported. Most companies have their own internal audit unit, which is reporting operational level fraud risks to CEO. Risk management and security functions are supporting fraud risk management or acting as risk consultants for other units. This is the case in most of the interviewed companies. The two subgroups do not differentiate from each other.

2.2. Does your company have an ethics policy, code of conduct or other guideline, which addresses fraud?

"The basis of the company operations is the compliance guideline and code of conduct. Other guidelines are building upon these. Fraud is not directly mentioned in those two guidelines, as they are more general in their nature. There are other guidelines, which do address fraud or parts of fraud such as bribery. If there are incidents, they are reviewed on a case-by-case basis in the compliance unit."

"Fraud is addressed in the security guideline. In addition, ethical principles address for example conflict of interests, communication guidance with external parties and relationships with vendors. Other examples are abuse of trust and position or negligence of internal guidance."

"There are separate guidances for fraud. Our values and HR politics supports code of conduct. There is guidance for disqualification, bribery and for fraud suspicion communication. COSO/ERM framework is not yet in use, but it has been presented to be implemented."

"Our ethical principles address fraud management. Also our values addresses fraud management as the content and meaning of our values is opened and explained to each line of business. General guidelines address the process of how to deal with fraud incidents."

"Bribery is clearly addressed and prohibited in our sourcing policy."

All the companies have guidelines addressing at least some frauds. Many companies use their ethical principles, company values or code of conduct guides as the basis of their business. Thus fraud is not necessarily directly mentioned in these guidelines as they are more general in their nature. However, fraud is mentioned directly especially in governmental agencies subgroup. Some of the companies have separate guidance and instructions for managing fraud. Some guidances addresses specific frauds and the processes how to deal with them.

Training and awareness program

2.3. Does your company give fraud prevention training to employees?

"Fraud prevention training is given on the topic of "the way we work". Training is continuous and it includes real fraud case examples. Training stresses the trust as a basis of the business, thus all fraud attempts are taken seriously."

"Managers are trained for risk management and security. Other employees receive fraud prevention training which focuses on the risks in their function, for example prevention of thefts."

"Fraud prevention and risk management is our substance of business. We provide training and it is open to all of our employees. Training is based on case examples and it includes going through of guidance. Topics in the guidance is discussed and explained in the training. It is the company's plan to systematically increase the knowledge of fraud prevention among the employees. Knowledge of fraud prevention among all employees reduces the possibility of social hacking. The more there is knowledge the harder it is to mislead our people. The goal for fraud prevention trainers is to spread the knowledge for others. In addition to the training there is guidance in intranet available to everyone."

"There are seminars for the key personnel about the current fraud related issues and about the processes and guidelines. Training of managers includes internal controls and risk management, therefore fraud management is part of that. Fraud prevention training is given in different occasions, sometimes in connection with other kind of training. We offer for example a six day risks management course, where our risk management experts provide the training. Risk management exercises in the training are suited to business needs, for example to exercises could cover payment transactions related risks."

"Our sales personnel are trained to manage frauds in their own area. In other areas, there are for example good guidances on investments and how to manage fraud there."

Fraud prevention training is supported in all interviewed companies according to the interviewees. However, the availability of the training varies from all employees training to manager or specialist specific training. Three out of five companies provided general risk management training, which is targeted to the management and to the key personnel. There are no differences between the two subgroups regarding this issue. In some companies, all fraud prevention and risk management training is open to all employees. In one company fraud prevention training is compulsory to all employees. The content of the training depends on the need. Typically employees are given fraud prevention training on a specific subject relating to their daily job.

Training is provided in seminars, classes or in company intranet in the form of e-learning. Seminars contain current fraud related issues, fraud management processes and guidelines. Real fraud case examples are typically used and the idea is to enhance employee's knowledge about fraud and corruption prevention. The more there is knowledge the harder it is to mislead our people stated one of the interviewees. Sometimes fraud and corruption prevention training is a subset of larger risk management training.

2.4. What kind of information about fraud you give to your personnel? (e.g. are detections made known, are employees informed about monitoring?)

"Employees are aware of the fraud incidents and attempts as they are used as case examples in the fraud prevention training."

"Fraud incidents are not communicated to the general public. Fraud incidents could be reported in the internal magazine. Use of fraud case examples in the fraud prevention training for management has been considered."

"If there is an inspection or audit then executives are aware of it. Some of the fraud incidents have been used in the training. There is an internal database of the fraud incidents and reports. Internal frauds are not usually published and communicated to other employees. However, all

fraud suspicions are reported and are taken seriously. Own business is reviewed analytically and the way of doing business is improved on the basis of the reports."

"Information is not given to everyone. Access to our fraud incident register is restricted to the team who deals with misuses and frauds. Managers are informed and they communicate possible cases in their team meetings. Fraud awareness communication to the employees stresses the controls and dangerous task combinations."

There are a lot of deviation in the way of communicating fraud management and incidents to employees among the interviewed companies. Some companies only emphasize the controls in the training, while other publish known fraud cases in intranet, newsletters and use them as case examples in the training. In the couple of interviewed companies, information is given to the management, who then in turn share the necessary information with other employees in the team meetings. Listed companies sub group is communicating fraud incidents more openly than governmental agencies.

Recognition

2.5. Do you monitor red flags?

"Red flags are monitored actively. Threats are followed closely, for example threats in the neighbouring countries. Experiences of threats and fraud incidents are communicated among the business. Active and daily communication with police is done in order to change information relating to incidents. Internally deviations from daily operations are monitored, so that even small hints could be followed. Communication between security, operations and external officials is open and active."

"Red flags are monitored. For example large financial transactions are reviewed. As the business functions are related together as a chain, red flags are also monitored through the whole chain."

"Red flags are randomly observed deviations, where attention is caught. Obvious red flags are followed intentionally. Projects are followed on the basis of reporting. Currently there is a project for risk management improvement and fraud risk management is part of it. Follow up

of red flags is done naturally as it belongs to the business and is part of the company culture. Some of the processes are standardized and accredited."

"Red flags are monitored in different levels. We use our own checklists and the results of the tests could raise the suspicions. Suspicions are checked by the information security group. Possible checking cases include money transactions with partners and travel expenses which are paid in the same day from different places. We are aware that there could be a risk in our system."

"No, we don't directly follow red flags."

Following of the red flags varies a lot between interviewed companies. In one company information gathering is not limited to the company itself, but it for example continuously monitors actions in the neighbouring countries. Fraud management actions are proactive in that company. This is enabled with good networks and communication between operative field, risk management, and officials. Communication is open and done through different channels. On the contrary, in one interviewed company red flags are not followed directly at all.

Most of the companies follow red flags on a reactive basis. They follow red flags in different levels and perform checks on a regular basis. Fraud attempts are usually monitored through official reports, surveys and reviews. In some cases, following of the red flags is done naturally, because it is part of the operations. There are no clear differences between the two sub groups of the companies.

Whistleblowing process

2.6. Do you use anonymous reporting eg. whistleblowing?

"Yes."

"Yes, there is a direct hot line. Anonymous reporting can be done also in the company intranet, through email or regular mail."

"Yes. Basically suspicions are reported to the own manager or manager's manager, but there is always an option to report to the security, internal audit or risk management department."

"It's not yet operational, but we have made an outline of the process. Currently possible fraud incidents can be reported to the direct superior."

Anonymous reporting process is in place in most of the companies. In many companies instructions states that reporting should be made to direct superior and if that is not possible then reporting should be done to manager's manager. Reporting to compliance, internal audit or security unit is also available in all companies. Multiple anonymous reporting channels are open, for example intranet, email, regular mail or phone. However, not all companies use anonymous fraud reporting. The answers of the sub group companies are very similar in this case.

Emotional aspects, motivation

2.7. Do you think working conditions have an effect to fraud prevention?

"Yes, working conditions have a significant effect to fraud prevention. If the working community is working, then it has a correlation to fraud prevention. For example possible employee's personal economic problems will be discovered early and managers can provide necessary support. Working atmosphere studies are organised annually. Working atmosphere is important so that employees feel that they can ask help if required. Good working atmosphere lowers the threshold to ask help."

"Yes, motivated employee trusts and respects employer."

"Yes. For example embittered employee might affect to the fraud prevention. Therefore we aspire to hear our employees. Naturally the realities need to be taken into account as everything is not possible. Employee well being is considered and thus our company provides a yearly job satisfaction query."

"Salaries compensate the working conditions."

All interviewees stated as their opinion that working conditions have a contribution to fraud prevention. Thus there are no differences between governmental agencies and listed companies. Two interviewees told that employee satisfaction is followed through yearly surveys. This is done in order to improve the working conditions. According to one interviewee, good working atmosphere provides better communication among employees. This enables asking help and thus decreases the cases of misunderstandings. Bad working conditions have an effect to fraud prevention. According to one interviewee, "embittered employee might affect to the fraud prevention". One interviewee stated that increased salary is one way to compensate working conditions.

2.8. Do you provide support, if employees have problems?

"Colleagues and managers can provide some sort of support, but occupational health care and security together can provide more support. Manager's role is to recognize employees who need support and provide support and guide them to the correct direction. It is their right and duty."

"Yes, basically occupational health care provides necessary support."

"Yes, those who need support are guided to the right place, for example to the occupational health care. Prime way to work through the employee problems is through support. Change of work task could be considered as well. Challenging HR issues are discussed in the management days. Alcohol or drugs haven't caused visible problems in our company. Internal frauds are difficult to accomplish due to the high level of security."

"Yes, it is done through our occupational health care."

All of the interviewees stated that support is provided, usually through occupational health care. Identification of an employee needing support is manager's responsibility stated two of the interviewees. Their responsibility is to guide employee to the right place, for example to the occupational health care. In one company it is possible to reassign responsibilities and thus help employees going through a difficult time. Priority in companies is helping employees.

Risks

Risk assessment

3.1. Do you classify and profile fraud risks regularly?

"Fraud risks are classified into internal and external risks. Internal risks are further classified into direct and indirect risks. Risks are classified based on their crime names. Risks are classified into groups based on damages frauds might be causing. As well, one risks classification is based on the source of risks."

"No, fraud risks are not classified or profiled regularly. Business areas prepare their own risk analysis and only if fraud stands up in the analysis, further action is taken."

"Yes, as it is the nature of our business. High risks are in a close follow up. We use traffic light classification of risks. That means that risks are divided into three different groups based on the severity of the risk. In internal risk management, risks are identified, reviewed and managed. However, the tools process is still incomplete, but the need for that is recognized."

"Board reviews enterprise wide risks on COSO/ERM basis. Line of business units prepares a SWOT analysis regularly and personal risk analyses are prepared when necessary. We have a risk management support group, which coordinates and develops the functionality of the risk management in a strategic framework. They check that risks are managed as a whole in the framework and then implement new risk management practises into the line of businesses. This unifies the risk management process in an enterprise wide level and brings synergy benefits. Fraud management guidelines and targets of controls are reviewed."

"We have built a list of frauds. We have a risk map, where we have estimated the probability and size of the impact. We have the used the process for one year now.

The method of classifying and profiling of risks varies somewhat between interviewed companies. Four out of five companies classify and profile fraud risks regularly. In one company actions to manage fraud risks is taken only if it stands up in the business area's own risk analysis. Both governmental agencies and listed companies classify fraud risks, thus there are no significant differences between the two subgroups.

Classification of the risks is based on crime names, damages, probability, severity and sources of risk. Division of the risks into internal and external is used in some companies. Further division into direct and indirect impact is used in one interviewed company. Enterprise wide risk management practises are adopted in almost all companies.

In one company internal fraud risks are divided into direct or indirect groups based on the way cost of fraud is incurred. In another company annual risk analysis preparation is based on SWOT analysis in an operational unit level. In the board level company risks are managed according to COSO/ERM principles. One company classifies external projects into three risk groups based on their total risk. High risks are followed up more closely than low risks. One company has mapped risks and uses risk scenarios. They have estimated the size of the impact and the probability of the event.

3.2. Do you prioritize fraud risks?

"Most obvious and most significant risks have been taken into account in the system design, so that tracking of the events and investigation is made easier. As the number of fraud incident in a year is small, in average ten incidents, there is no reason to prioritize a single fraud risk. The base principle in prioritizing is that when incidents are noticed in the risk environment they are communicated quickly so company can prepare to the possible threat. As there have been so few fraud incidents, company has not made any statistical analysis on them. Most of the known fraud incidents have come from outside of the company. Our personnel are honest and risk aversive."

"No, we don't"

"Our company uses the traffic light model for prioritizing risk. Green light means low risk and less follow up. Yellow light indicates moderate risk and some follow up. Red light points to high risks and those risks require special follow up. Internal risk are planned to be prioritized on the basis of each risks likelihood and impact."

"In the strategic planning head of the company prioritizes risks and currently they see image risk as the most significant fraud related risk."

"Yes, there is a priority order. Firstly we must secure our guidances."

Three of the interviewed companies prioritize fraud risks and two of the companies treat fraud risks equally. Interviewed companies prioritize fraud risks in the strategic planning, use the traffic light model or mapping. However, one interviewee stated that the amount of frauds in a year is so small that there is no reason to prioritize a single fraud risk. They are rather preparing for the risk whenever it is noticed. Two of the interviewed companies manage all possible fraud incidents as separate cases. Governmental agencies subgroup is prioritizing fraud risks more than listed companies.

Risk treatment

3.3. To what extent identified risks are avoided, reduced, transferred or accepted?

"We intend to avoid identified risks by processes, which prevent fraud. Risks are reduced through employee training and guidance. Employees are for example instructed to contact security department when they have any suspicions. Identified risks are also reduced through outsourcing. Outsourcing has been based on the risk analysis. For example we use trained guards to enhance the security of the premises. As well, we use external lawyers whenever required. However, fraud risks cannot be transferred as in the end of the day they are regarded as our risk. As all of the risks cannot the avoided, reduced or transferred, thus they must be accepted."

"Our aspiration is to prevent possible fraud incidents. Prevention is done through controls. Some of the risks are transferred through indemnity insurance. As 100 % control are impossible, therefore controls should not be too heavy. Controls are based on four eyes principle, so that no one can act alone. Payments are monitored closely and we consider that business flexibility is important."

"Damaging, unnecessary risk taking is not tolerated. If the return is not adequate compared to the risk, then it is avoided. Risks are reduced through inspection of high risk areas. High risk areas are reviewed more often than low risk areas. In our business transfer of risks is not possible. Some risks in the short term financial arrangements are accepted as complete control of risks is impossible."

"Lines of businesses concentrate on avoiding and reducing of the risks through controls and specific risk related actions. Controls are not in every detail at the adequate level in all units."

"If we notice an incident which has happened more than once, then we must act. We use several methods to avoid and reduce the possibility of fraud. The risks are not necessarily transferred to the third party in every business. However, we have an insurance against stealing and shoplifting."

Naturally all companies try to avoid unnecessary risk taking. If the return to risk ratio is too low, then the project is avoided. Companies try to avoid identified fraud risks with risk management processes, such as controls.

Risks are reduced through employee training and guidance. Outsourcing was mentioned as one mean of reduction of the risk, for example through the use of external lawyers in complicated contract issues and trained guards in the premises security. Open communication and cooperation with stakeholders is used to reduce the risk. As well, inspections of the high risk areas are mentioned as risk reducing methods. Specific risk management practises are targeted to specific fraud risks thus reducing the total fraud risk.

Two interviewed companies use insurance to transfer some specific fraud related risks, for example through use of indemnity insurance or theft and shoplifting insurance. Intangible fraud risks are not fully transferable according to one interviewee, in the end they are always company's risks.

As all risks cannot be avoided they need to be accepted. Additionally, too heavy controls may burden the business, especially when flexibility is needed. The subgroups are not differentiation clearly from each other. All of the companies are trying to avoid and reduce the fraud risks.

Implementation of controls

3.4. To what extent identified risks are controlled through preventing, deterring and detecting measures? For example, do you screen employees at the recruiting phase?

"Risks are controlled using two approvers for transaction. Monitoring of the risk environment is important. Security and risk management is learning from the past experiences. If there has been a fraud incident, systems are reviewed, loopholes are fixed and new guidelines are set up in order to prevent further incidents."

"Employee's personal characteristics and suitability are tested in the recruiting phase. Plans for training and education are acting as preventing measures. Working time control is used in our company. Premises and access control is used as well. Systems are secured well and emphasis is put on the secure data transfer. Job descriptions are planned, jobs are separated and plans are followed up. Therefore they prevent and deter dangerous task combinations."

"Risks are managed through controls, open communication and training. In the recruiting process candidates skills and style is reviewed, as well as their work history."

"We're checking the backgrounds of those managers, who have the underwriting right. We have put in place many measures of controls."

Mentioned preventing measures include working hours follow up, premises and access control, systems security, training and education, work chain screening, project planning and follow up. Many companies require two different approvals for all transactions. Employee screening in the interviewed companies include the suitability, skills and style tests.

Separated job task and removal of dangerous task combinations act as deterring measures. Detecting measures are used and if fraud is revealed, actions are taken. Those actions include review of controlling systems, improving controls and guidelines.

Risk follow-up

3.5. How often you update risk profiles?

"As we haven't yet formed our risk portfolio, enterprise wide profiles cannot be updated. However, some departments update their own risk profiles, for example IT department is updating risk profiles continuously. Customer database is updated continuously. Changes in the projects are followed. Follow up is based on the severity of the risks. Internal risks are not followed up as there isn't a process for it. However, the need for that kind of a management

tool is recognized. Board is updated of the broad risk entities, such as globalisation including knowledge transfer, reputation and personnel issues like aging, education level, health and safety and competitive ability. Board is informed about the possible uncontrollable strategic risks. Our processes are already designed to correct and manage small risks, which are not strategic."

"We put our emphasis in risk profiles to the large and demanding risks, which are strategically significant and require analysis and guidance. For example the basis of our business is responsibility. If we do not do business in a responsible way, it is a strategic risk and affects the guiding of the business. Another example is personnel risk. Diversity and agility of our personnel is strategically important."

"Risk profiles are updated on a yearly basis. Risk management plans and results are reviewed every six months by the internal audit. Board reviews current risks reported by the leadership team on a monthly basis and react immediately to the threats. The process is systematic and planned. We could react to specific risks on a daily level. Fast reaction is crucial. Our managers are committed to the risk management. The risk management guidelines and processes are uniform across the businesses and the results are benchmarked. Results of the risk management are tied to the reward program."

"We haven't updated our risk profiles."

Update of risk profiles varies greatly between interviewed companies. In one interviewed company, existing profiles are not updated. Another company has not formed the risk profiles, thus they cannot be updated. However, preventive measures are used and reporting of the risks is done regularly on broad issues like globalisation, IT security, transfer of know how, reputation, aging of personnel, employee education level, health & safety, competitiveness and uncontrolled risks.

In another interviewed company risk profiles are updated at least twice in a year in a systematic way. Identified risks are managed immediately. As well, risks are reviewed on a monthly basis in a board level. Quality of the risk reviews are measured between operational units and these measures are linked to reward program.

One company stated as well, that risks are managed immediately. According to the interviewee it takes approximately one hour to update all relevant persons of the new fraud risk after it is identified. Protective preparations are started immediately after identification of risk. This risk does not need to be inside the company or threatening the company. Risks are scanned continuously from different sources, countries, inside and outside the company. There is not a clear distinction between the two subgroups of companies regarding this question.

Monitoring and detection, red flags

3.6. Do you monitor your employees, if they have undeclared involvement in companies, erratic behaviour (gambling, misuse of alcohol) or misuse of expenses?

"Employees are not monitored."

"Our internal audit team has couple of tools to check employee expenses. Audit is done to random employees."

Employees are obliged to inform their involvement in other companies in one out of five interviewed companies. Some business operations, such as consulting of the customer need specific permission from the company. One company checks randomly employee use of expenses. Two interviewed companies do not monitor employee related red flags at all. Governmental agencies subgroup is putting more emphasis on employee monitoring than listed companies subgroup.

3.7. Do you monitor transactions, i.e. do you have payments to tax havens, tied suppliers, sales at excessive discounts?

"Yes, large transactions are monitored. In order to prevent tied suppliers incidents, different buyers are used."

"Employees have an obligation to notify security or risk management department if they notice suspicious transactions. As transactions data is visible, it is difficult to misuse the system without being noticed."

"We review transactions on the headline level. Transaction review is in the discussion of the risk management."

Most of the interviewed companies monitor large or suspicious transactions. One company uses different buyers to prevent tied suppliers issue. Employee notification of suspicions is also used according to one interviewee.

3.8. Do you monitor your systems? For example, is there systematic abuse of procedures, unusual emails, misuse of passwords?

"Some of the systems have access control and they are monitored. IT department follows logs, error notifications and network usage. Firewalls are used and followed."

"We have spam filters in use and our IT department monitors our systems. For example, we follow the time used in internet surfing."

Deviations from normal operations, attacks against IT systems and follow up of the activities in the net are measured in couple of the companies. Logs and error notifications are used in the measurement process. Network usage is followed as well. There are no differences between the two subgroups of companies regarding this question.

3.9. Do you audit corporate level risks? Are there over-zealous acquisitions strategies, artificial barriers put up by directors to avoid questions, increased concerns raised by regulators or weak management?

"Internal audit monitors actions of the management. Internal audit function cooperates with the risk management function."

"All acquisition related decisions are brought to board level. As well, we have a corporate wide credit control policy."

This question was not bringing much discussion from the risk management experts. One interviewee stated however, that all their acquisitions are brought to board level. Internal audit

monitors actions of the management in one company and at the corporate level, credit control policies are reviewed regularly at least in one company.

3.10 To what extent your company uses processes designed to detect, investigate and resolve proactively potentially significant fraud? For example use of fraud detection tests.

"Company uses processes to detect over-sized transactions."

"New systems are built to audit business continuously. This system will be a risk based system. Tests are used to review the processes."

"Company is audited by external auditors. Our internal audit team has a role regarding the responsibilities."

"Corporate level risks are audited by the line of business management. The management processes and controls are in place."

Detecting measures are used in many interviewed companies and most of the interviewed companies have an investigation team, which aim to investigate and resolve frauds. One interviewee stated that they are building a risk based system, which would audit business continuously. None of the interviewees mentioned fraud detection tests. The governmental agencies are putting more emphasis in their answers to external auditing than listed companies.

Managing incidents and follow up

Incident management and reporting system

4.1. In what ways fraud incidents are managed and reported in your company?

"Both internal and external incidents are recorded in the system and they are reported to the management in a general level. If same person is caught again in a fraud attempt, the case will be taken to the court. An internal incident leads to the discussion with the management. Company tries to understand how the incident happened by gathering all related information in an objective way. Rights of the suspect are taken into account, for example information gathering and judgement making are separated functions. Company tries to minimize

damages; therefore for example systems are reviewed in order to prevent further incidents. Company tries to learn from the incident. External incidents are routed to the centralised security department and not to the operational unit."

"If someone is suspecting a fraud, employees are instructed to contact unit's security manager. Operational unit is not allowed to investigate possible fraud case alone. Security department is in charge of investigation. Reporting is done to the executive management and to the operational unit where possible case is located. Development of the investigation is reported also to the middle management."

"Possible fraud cases are managed on a case-by-case basis. Reporting is based on the professional report. Fraud management guidance is being prepared as management consideration in the fraud incident situation is not always regarded sufficient. All external fraud incidents are reported to the police. Company co-operates with audit companies in fraud incident situations. Together they analyze the current situation, act upon the standards and report to the necessary authors. Low profile is kept during the investigation phase, so that evidence is not lost. Company uses professional help in investigation."

"We have our own developed process for our employees and for our customers. There is a guideline for customer related fraud cases. The level of detail of the fraud data varies, but we gather statistics of the frauds from our business lines and from our units. We have a time series, where we try to find out which factors affect to the frauds. Our processes are audited."

"We haven't had any significant frauds in our company. If something happens, then managers of lines of businesses are responsible for the communication."

Management of fraud varies considerably among the interviewed companies. There are not many similarities inside the subgroups of companies. Most of the companies have comprehensive processes and guidelines for the possible incidents, some are using more external help while other are centralising the investigation. At least one of the processes is audited. Two of the interviewed companies record all incidents for investigation purposes. Suspicions are instructed to report to the security or risk management department in some interviewed companies. In two of the interviewed companies, operational units are not allowed to investigate the incident alone. Instead investigation responsibility is given to the

security department. Low profile is preferred in the first phase of the investigation so that evidences are not lost. Purpose is to get as much information as possible and to prevent further damages. One interviewee stated that they could use external specialists. Another interviewee stated that they try to understand how the incident has happened and learn from the incident. In one company information gathering and judgement process are separated in order to protect the rights of the suspect.

Reports from the fraud are prepared for the management in most of the companies. Some companies inform management in the place of the incident. Development of the investigation is also reported. One company prepares broad level fraud reports to EU. All of the interviewed companies report external fraud incidents to the police, thus in that sense sub groups of the companies are similar. Companies try to provide as much investigation material to the police in order to help and speed up the police investigation.

4.2. What would be the most severe fraud impact to your company?

"Reputation risk is the most significant risk. Small monetary losses do not harm business as much as for example possible news headlines of money laundering. Reputation has implications to the internal and external environment. Reputation has an effect to the trust of the employees. Damaging news could affect negatively to the share price."

"The amount of losses in a severe fraud case could have 10 – 100 million euro impact to the profit. Fraud incident might cause losses in the reputation. Fraud incident could negatively affect the prerequisites for business operations and therefore cause decline in the share price. If there has been a large scale fraud incident, then it requires major improvements in the systems. Therefore investigation costs could become significant in major improvement projects. Not all of the costs are caused by the investigation. Risk management and improved controls contribute to the total costs."

"The most severe fraud impact is lost of reputation. For example if customer's data ends up in wrong hands, it is causing a big damage to our reputation. Classified customer information in the wrong hands could lead to significant monetary losses. Loss of reputation could threaten the existence of the whole company and also the whole Finnish economy."

"Image risk through bad publicity from the fraud case. It could lead to credibility risk. Hypothetical example is that employee or manager uses the funds of the company to their own purposes."

"Lose of reputation, which negatively affects our share price. For example, if an unmanageable fraud incident would reveal, that would cause reputational losses."

All of the interviewees stated that image and reputation risks cause most significant impacts to the company. Ruined reputation decreases trust to the company and this can endanger the whole existence of the company or at least reduce the share price. One interviewee estimated that a severe fraud can cause 10 to 100 million euro costs. However, most of the interviewees said that fraud do not create a significant financial risk. Additionally, improvement and fraud review costs can become significant in large security improvement projects.

4.3. What kind of impact creates, according to your opinion, most significant threat to your company, tangible or intangible costs?

"Intangible risks are most significant, as the incident don't need to be big when it's already affecting business."

"The probability of the risks are larger in tangible costs, therefore tangible costs are causing most significant threat. Indirect costs are significant in large fraud incidents. In small fraud incident indirect costs may become larger than direct losses from the incident."

"Intangible costs are most significant."

"Intangible costs are most significant to us. As we're operating on the basis of trust, therefore, frauds could threaten the ethics, equality and trust. Therefore it could threaten the existence of our company."

"Intangible costs due to reputational risk are the most significant costs."

Four out of five of the interviewees stated that intangible costs are most significant costs. This is because losing of trust and reputation can cause severe damages, for example they can

endanger existence of the whole company. However, one interviewee stated that tangible fraud costs can become larger than intangible costs as the probabilities of the risks are larger for tangible costs. One interviewee stated that in small fraud incidents, indirect costs may become larger than direct fraud costs. The answers of the subgroups are similar.

Fraud response plan

4.4. Does your company have a fraud response plan?

"Fraud response process is described and is available in the company intranet. For example fraud response plan states that company responses to all external crimes against the company."

"No."

"In the different company level there are some response plans, for example communication plan. However, as the situation in fraud incident is very unclear, it is difficult to prepare a response plan."

"Yes, we have a fraud response plan. It is very detailed and it's available in our company intranet. The plan is tied to our ethical principles, enterprise wide risk management principles and to the operative management. The plan is intended to cover the whole enterprise."

"Yes. We have a planned incident investigation process."

Three of the interviewees stated they have a fraud response plan. Only one interviewee stated that they have a very detailed plan. One of the plans covered only investigation process. On the other hand two of the interviewees said they don't have a fraud response plan. Reason for this was that frauds are so different that it is difficult to prepare for them. There are no similarities of the answers inside the subgroups, thus there is no clear difference between the subgroups regarding this question.

Qualified investigation team

4.5. Which kind of authorities you contact when a fraud incident is revealed?

"If the incident is crime then company contacts police, their law office and financial supervision authority."

"If there is a doubt about possible fraud incident, security unit is gathering evidence of the crime. Company contacts police if they suspect fraud. All crimes are reported to the police. If required, private detectives could be used. Forensic services consultants could be used depending on the case."

"In severe fraud incident we contact our audit company, police and other required authorities. We co-operate with central criminal police, customs and Finnish governments grey economy investigation group."

"We contact police, prosecutor and justice of court. In addition to that we contact our partners, tax authorities and other government authorities."

"We contact police."

All of the companies would eventually contact police. One company would contact police after preparing all the necessary documents for them. Other authorities included auditors, tax authorities, financial supervision authority, central criminal police, prosecutor, ministries, customs and Finnish governments grey economy investigation group. Some interviewees stated that they might contact private detectives or forensic services consultants. Governmental agencies report fraud incidents to many places, while listed companies tend to report mainly to the police.

4.6. Do you have internal fraud investigation team?

"Yes, company gathers material for the police, for the court and for the prosecutor. This speed up the process, thus the case could be prosecuted faster. This improves the likelihood of the recovery from the incident. Company management, communication department and authorities are informed during the investigation. If the incident is not regarded as crime then operational units could manage the incident independently."

"Yes, security unit. In group level, there are two persons in the team. In the branch level, there are five people in the team."

"Internal fraud investigation team is gathered on case-by-case basis, but we don't have an official internal investigation team."

"Yes, there exists an internal fraud investigation team. The members of the team include the leader of the unit, lawyer, internal auditor and an expert on case by case basis. Light structure of the team enables the team to act rapidly. They have a possibility to hear other parties of the case."

"Probably we have a team...Responsibility of the investigations is in line of business management."

All of the interviewees stated they have a fraud investigation team, although in some companies it is gathered on case by case basis. All of the teams are rather small, containing for example managers from the unit where the incident happened, company lawyer, internal auditor and case base expert. Light structure of the team enables the team to act rapidly according to one interviewee. The aim of the investigation team is gather material for the police, for the court and for the prosecutor in order to speed up the investigation and prosecution process. According to one interviewee this improves the likelihood of the recovery from the incident.

Follow-up and sanctions

4.7. What kind of sanctions is used to punish fraudsters?

"Sanctions range from written or verbal notification to warning and to ending the employment contract. Incident regarded as a crime are always reported to the police. This information is available in the company intranet is open to all employees. Sanctions are based on the law and law offices are consulted when necessary. HR management can decide of the sanctions and they can consult compliance unit."

"Sanctions are based on the employment contract law. Sanctions vary from warnings to termination of employment contract."

"Sanctions follow the law. If employees are found doing a fraudulent act, they could be suspended."

"We have our HR guidance, where we have made marked the boundaries of fraud and mistakes. If the incident is mild, we give a reminder or warning. If the incident is severe, then we cancel the employment contract and report the case to the police. The punishments vary depending on the fraud severity, but punishments are always done according to the law."

"It depends on the case as the incidents vary from dismissing employees to change of tasks. Depending on the issue, we could take the incident to the court."

Sanctions depend on the severity of the case, but they are always done according to the law. They can vary from serious to light, from police investigations, cancelling work contract, returning the benefits and covering the costs, changing of the work tasks to warning, reminder and written or verbal notification. Sanctions are based on the law and court order. Decision between serious and light incident is done based on the HR guidance in one company. Employee rights are respected and taken into account. All interviewees stated that crime incidents are reported to the police. The sanctions are not different among the two subgroups.

System follow-up and recovery

4.8. How fraud could affect your systems and what kind of measures should be done in order to recover from the losses fraud incident caused?

"Company has a business continuity plan, which contains recovery plan and crisis management plan. Fraud incident cases are reported and necessary system changes will be done to prevent further incidents. System changes causes expenses thus these are taken into account when planning the new system. Necessary guidance and training is provided to the personnel when system changes are made. Processes are reviewed and amended to prevent further incidents."

"Company investigates how to prevent further incident going forward. System design is reviewed in order to find out if it could be improved. The owner of the system is responsible

for making control improvements. If fraud incident has happened, control improvements are suggested and their effectiveness is reviewed after implementation."

"Critical information technology data could be restored quickly. However, it is more difficult to recover from the losses of key personnel."

"For example, if we discover a misuse of our systems, then we need to change our controls. We need to review the controls and suggest improvements. If we discover one misuse then it's possible that other systems are also vulnerable and thus those need to be reviewed too. If we change the controls, then we need to update our guidelines and red flag checklists."

"We would need to change our guiding systems and build more controls into it, if fraud is revealed. We would need to remove dangerous task combinations by changing the tasks of the employees."

After possible fraud incident systems, processes and guidance are changed in all companies to avoid such abuse in the future according to interviewees. Losing of key personnel is hard to recover according to one interviewee. On the other hand, system recovery is easier. After possible fraud event, systems are investigated and reviewed. Then improvements of control enhancements are investigated, evaluated and implemented. Implementation includes guidance and training of the employees. After implementation of controls their function is reviewed.

Management review of incidents

4.9. What kind of measures is taken in order to enhance company's ability to manage fraud risks?

"Company has a report of events and incidents for the operative risk management department. They provide management possible threat reports so that proactive measures could be made. As the company operates in several countries, there are country specific differences in the valuation of different risks and threats. This has implications to the report given to the group management, as risks are not seen similarly in all countries. Thus company has increased communication between risk specialist and understanding of the culture in order to have understanding of the country specific risks. This has lead to enterprise wide risk guidelines."

"Company has adopted controls in the payment transactions. Company has transferred risk to the insurance company by taking theft insurance. Internationalisation is taken into account and company has prepared for the criminal activity. The importance of the information systems is growing, thus emphasis is put in the IT security. Therefore information management and risk management is working closely together."

"Risk management should be developed even further as fraudulent acts could cause significant risks. Our company provides yearly fraud risk and legal risk report to the board, which in turn reviews the report."

"We have planned the responsibilities of the risk management. We have used an enterprise wide risk management practises. Our emphasis is in information systems and in process description and process development. Our board sees the risk management as a part of the business, which is interlinked to other functions and profit seeking."

"We have started an ERM project, which aims to unify our risk management processes in the company. Our biggest risks currently relate to guidances, reporting and project tracking according to our audit committee. It is our aim to unify the management of these risks as a part of the normal operations management."

Three of the interviewees stated they are concentrating in the improvements of enterprise wide risk management and interlinking risk management in other functions and profit seeking. One interviewee stated they have put emphasis on development of IT systems as it is getting more and more important. According to that interviewee, information and risk management are now working closely together.

Two of the interviewees from the listed companies' subgroup brought up internationalisation, differences in the values and interpretation of risks and threats. One company puts emphasis on communication between risk specialists in different countries. According to the interviewee, this has led to enterprise wide risk guidelines. Another interviewee emphasized the preparation against the international criminals. Governmental agencies subgroup is not talking about the international fraud risks.

One of the companies has transferred part of the risks to the insurance companies. Two of the interviewees said they provide reports to the board on current events and incidents so that management can proactively seek new solutions.

5. Conclusion

Results of this study are divided into the three groups, to risks, prevention, and to recovery following the theme in this study. In general the two subgroups of the companies, government agencies and listed companies do not have many differences in the answers. However, six out of 29 of the questions give clearly different answers between the two sub groups. If there are differences between the two subgroups, they are mentioned in the results.

5.1. Results

The main findings of the three fraud costs elements are that companies have a good sense of what fraud means in their respective business. All of the companies have some sort of guidance or policy, which states fraud, thus fraud risk is recognized in the companies. This result is different compared to Vähäkuopus (2004) study. This means that companies have recognised fraud risk only recently or the selected companies in this study are well aware of the fraud. Guidances and policies addressing fraud bring transparency to the fraud management practises.

Fraud is criminal activity, which is intentional and planned according to the interviewees. This is in line with the fraud definition used in this study and with other definitions presented earlier in this study. Fraudsters try either benefit or cause damages. However, there was deviation in the definitions. The definition varies internationally from country to country. Interviewees stated that fraud risk is a significant risk, which is usually related to non-monetary, soft items, such as reputation, image or customer relationships. This is in line with Vähäkuopus (2004) study. Companies consider also their stakeholders when valuing the risk.

All of the companies had recognized the fraud risk and most of them regarded it significant. One sign of the true significance of the risk is that they all provide fraud prevention training to their employees. Thus the risk is taken seriously. The availability of the training varies between companies, in some companies training is open to everyone, but on the other hand in some companies training is provided only regarding a specific fraud type relating to the job.

Regularly held training seminars usually contained real life fraud case examples. As well, all of the company representatives stated that working conditions have an impact to the fraud prevention, thus opinion surveys are held annually in many companies to get ideas of improvement areas. Additionally all stated that their occupational health care provides necessary support for those employees who require it.

Companies use various methods at different levels to prevent the fraud risk, which they regard significant. Three out of five companies prioritize their fraud risks and two out of five treat them equally. Government agencies prioritize different fraud risks more than listed companies, which mainly treat them equally. All of the companies avoid unnecessary risks and try to reduce those risks which cannot be avoided through training and guidance, outsourcing and specific inspections to high risk areas. According to the interviewees, fraud risks are difficult to transfer to other party as they are usually relating to intangibles. However, companies use insurances and have outsourced some fraud risks. Interviewees argued that as it is impossible to control all fraud risks, thus some of them have to be accepted. As companies are there to make profit, they need to take some risks as well. All of the companies are reducing fraud risks through various means of controls at different levels, such as authorisation of the payments, system build in security, or project follow up.

One of the interviewed companies manages risks proactively, while rest of the companies manages them reactively. Notably, two of the interviewed companies do not claim to follow any red flags. Those who follow red flags, concentrated merely on the large transactions or high risks areas. However, government agencies are monitoring employee related red flags more than listed companies. As well, government agencies tend to put more emphasis on external audit than listed companies.

According to the interviewees' opinions the most significant fraud risk is reputation related. As the lost of reputation could endanger the whole existence of the company. One interviewee estimated that the total fraud damage can be from 10 to 100 million euro. As well, most of the interviewees stated that frauds do not usually pose a direct financial threat to them; instead it is causing indirect and intangible costs. One interviewee said that indirect costs can be even higher than direct fraud damages as they need to review and implement new prevention systems, change their processes and update guidances. This result is in line with Vähäkuopus (2004) study.

Recovery from fraud incidents depends on the incident management, availability of the response plan and investigation team, as well as sanctions and follow up processes. New fraud risks are reported to the executive management or board either regularly or whenever they arise. Executive management is responsible of the fraud risks at the end of the day, even though follow up of the risks can be brought down to all employee level.

Communication and management of the frauds varies between companies. Some inform the frauds to all personnel for example in the internal newsletter, while others provide information of the fraud incidents only to the management. Listed companies stated to communicate more openly fraud issues to the employees than government agencies. Management of fraud risks differs in investigation and reporting practises. For example one company separates the information gathering and the judgement of possible fraudster to protect the rights of the suspect. Common thing in investigation is the low profile information gathering for the police to speed up the investigation process. Only three out of five companies stated they have some sort of fraud response plans. Two of the interviewees stated they do not have plans because the possible fraud incidents differ so much from each other and thus it is challenging to prepare for them. However, all of the companies would contact a police in case of fraud. Government agencies report fraud incident to several instances while listed companies contact mainly police. Interviewees stated that frauds that are regarded as a crime will be prosecuted. Sanctions to internal fraudsters varied from verbal or written warnings, change of task to dismissal of the job and prosecution.

Risk management practises are improving in all of the interviewed companies. Three out of five companies is working on the enterprise wide risk management system implementation to enhance the company against risks. Interviewees stated that other fraud risk management improvement areas are IT systems, information management, closing of international fraud information gaps and preparation against the international criminality. Government agencies are not bringing up the international fraud risk threat while listed companies are preparing for it. International operations can be one reason for this.

5.2. Future research

This area of study is not well covered by researches. It is a new area of study as the concept was first defined in 1939 by Sutherland. Regardless the fraud risk management is relatively

new area of study, it is worthwhile to study as it can bring significant benefits to the companies risk management practises. This study illustrates the breakdown of the total fraud costs and the notes the linkages between these cost elements. Future research on the related subject can be done on the linkages between the cost groups. That study could point out where the correct balance of prevention to fraud risks is and how much emphasis can be put on the recovery. Other future studies can dig even deeper in these three fraud costs and discover which factors contribute to these elements and how those factor can be managed better. Third suggested future research on this topic would be an international comparison of the risk managers' perceptions on total fraud costs.

REFERENCES

Albrecht, W.S., Wernz, G. W., 1993. The three factors of fraud. Security Management 37:7, Arlington, Jul, 95-96.

Alvesalo, A., 1998. They Are Not Honest Criminals, in Organised Crime & Crime Prevention - What Works, Rapport fra NSfK´s 40. forskeseminar. Espoo, Finland 1998, Copenhagen: Scandinavian Research Council from Criminology.

Alvesalo, A., Tombs, S., 2004. Economic Crime Control in Finland. Sociology. Vol. 38 (1), 165-174.

Association of Certified Fraud Examiners (ACFE), 2004. Report to the Nation on Occupational Fraud and Abuse.

Association of Certified Fraud Examiners (ACFE), 2002. 2002 Report to the Nation. Occupational Fraud and Abuse.

Association of Certified Fraud Examiners (ACFE), 1996. Report to the Nation on Occupational Fraud and Abuse.

Basel Committee on Banking Supervision, 2003. Overview of the new Basel capital accord. Basel.

Cloninger, D. O., 1982. Moral and systematic risk: a rationale for unfair business practice. Journal of Behavioral Economics, 33–49.

Cloninger, D. O., Waller, E. R., 2000. Corporate fraud, systematic risk, and shareholder enrichment. Journal of Socio-Economics 29:2, 189-201.

Comer, M. J., 1998. Corporate Fraud. Gower Publishing Limited, 3rd ed, Brookfield.

Commission of the European Communities, communication from the commission to the council and the European parliament, 2003. Modernising company law and enhancing corporate governance in the European Union – a plan to move forward (action plan), 21.5.2003, COM (2003) 284 final, Brussels.

Committee of Sponsoring Organisations of the Treadway Commission (COSO), 1992. Internal control, integrated framework.

Criminology Mega-Site, http://faculty.ncwc.edu/toconnor/criminology.htm, 17.12.2005.

Davia, H., 2000. Fraud 101: Techniques & Strategies for Detection. John Wiley & Sons Inc.

Ernst & Young (E&Y), 2003. Fraud, the unmanaged risk, 8th global survey. http://www.ey.nl/download/publicatie/8th_Global_Survey.pdf, 24.2.2004.

Ernst & Young (E&Y), 2000. Fraud, the unmanaged risk, an international survey of the effect of fraud on business.

http://www.ey.com/global/download.nsf/UK/Fraud_2000_Survey/$file/FraudSurvey.pdf, 23.2.2004.

Finnish Government, 1996. Action Programme of the Finnish Government to Reduce Economic Crime and Black Economy, Helsinki.

Fooks, G., 1999. The serious fraud office: policing the city or policing for the city. Paper presented at the British criminology conference, Liverpool, 13-16 July.

Green, S., P., 2004. The concept of white collar crime in law and legal theory. Buffalo Criminal Law Review 8, No. 1.

Heiskanen, V., 2006. Cost and likelihood of corporate fraud. Master's thesis, Helsinki School of Economics.

Institute of Directors in Southern Africa, 2002. Executive summary of the king report 2002.

Institute of Internal Auditors, 2007. http://www.theiia.org/guidance/standards-and-practices/professional-practices-framework/standards/standards-for-the-professional-practice-of-internal-auditing/?search=glossary&C=816&I=2343, 17.10.2007.

Jokinen, A., Häyrynen, J., Alvesalo, A., 2002. Yritykset talousrikollisuuden uhreina. Poliisiammattikorkeakoulun tiedotteita 19. Edita Oyj, Helsinki.

Keskuskauppakamari ja Helsingin Seudun Kauppakamari, 2005. Yritysten rikosturvallisuus 2005: riskit ja niiden hallinta. Helsinki.

Killick, M., 1999. Fraudbusters. The inside story of the serious fraud office, London: Indigo.

KPMG, 1995. Airline fraud survey.

KPMG, 2003. Fraud survey 2003. http://www.us.kpmg.com/RutUS_prod/Documents/9/FINALFraudSur.pdf, 24.2.2004.

Krambia-Kapardis, M., 2002. Fraud victimisation of companies: the Cyprus experience. Journal of Financial Crime 10:2, 184-191.

Levi, M., 1993. The investigation, prosecution and trial of serious fraud. The Royal Commission on Criminal Justice. Research Study No. 14, London: HMSO.

Nettler, G., 1991. Crime in America. Economist, 00130613, Vol. 319, Issue 7701. 6 April, 1991.

Norwegian Government, 2004. The Norwegian government's action plan for combating economic crime. Oslo.

PricewaterhouseCoopers in association with Wilmer, Cutler & Pickering (PwC), 2003. Global economic crime survey 2003. www.pwc.com/crimesurvey, 24.2. 2004.

Ramsay, I., 2001. Independence of Australian company auditors: review of current Australian requirements and proposals for reform. Commonwealth of Australia.

Reichert, A. K., Lockett, M., Rao, R. P., 1996. The impact of illegal business activity on shareholder returns. The Financial Review 31:1, 67-85.

RSM Robson Rhodes LLP, 2004. Economic crime costs UK PLC 40 billion a year. http://news.bbc.co.uk/2/hi/business/3751160.stm, 17.10.2004.

Samociuk, M., Iyer, N., Lehtosuo, K., 2004. Väärinkäytösten Torjunta – Käytännön Opas. Gummerus Kirjapaino Oy, Jyväskylä, 1st ed.

Samociuk, M., Iyer, N., 2003. Fraud Resistance – A Practical Guide. Strategic Value Management Series. Standards Australia International limited, Sydney.

Schwendinger, H., Schwendinger, J., 1975. Defenders of order or guardians of human rights. In: Taylor, I., Walton, P., Young J. (Ed.), Critical Criminology, pp. 113-46. London, Routledge & Paul, K.

Sellin, T., 1938. Culture conflict and crime. NY: Social Science Research Council.

Slapper, G. and Tombs, S., 1999. Corporate Crime. London, Longman.

Snider, L., 1993. Bad Business: Corporate Crime in Canada. Scarborough, ITP Nelson.

Snider, L., 2000. The sociology of corporate crime: an obituary (or: whose knowledge claims have legs). Theoretical Criminology 4, No.2, 169-206.

Sutherland, E. H., 1940. White-collar criminality. American Sociological Review 5, 1-12.

Sutherland, Edwin, 1949, White Collar Crime. Yale Univ. Press, New Haven.

Tappan P., 1947. Who is the criminal. American Sociological Review, 12, 1, 96-102.

The Institute of Chartered Accountants in England and Wales, 1999. Internal control: guidance for directors on the combined code (Turnbull report).

The Institute of Internal Auditors (IIA), 2004. International standards for the professional practise of internal auditing. http://www.theiia.org/iia/index.cfm?doc_id=1499, 2.3.2004.

Transparency International, 2007. 2007 Corruption Perceptions Index press release. http://www.icgg.org/corruption.cpi_2007_pressTI.html, 26.9.2007.

US Congress, 2002. Sarbanes-Oxley Act of 2002.

Vähäkuopus, E., 2004. Fraud risk management in Nordic companies. Master's thesis, Helsinki School of Economics.

APPENDIX

Interview questions

General questions

1.1. How do you define fraud?

1.2. How important you regard fraud risk?

Prevention

Tone at the top

2.1. Who is responsible for managing fraud in your company?

2.2. Does your company have an ethics policy, code of conduct or other guideline which addresses fraud?

Training and awareness program

2.3. Does your company give fraud prevention training to employees?

2.4. What kind of information about fraud you give to your personnel? (e.g. are detections made known, are employees informed about monitoring?)

Recognition

2.5. Do you monitor red flags?

Whistleblowing process

2.6. Do you use anonymous reporting e.g. whistleblowing?

Emotional aspects, motivation

2.7. Do you think working conditions have an effect to fraud prevention?

2.8. Do you provide support, if employees have problems?

Risks

Risk assessment

3.1. Do you classify and profile fraud risks regularly?

3.2. Do you prioritize fraud risks?

Risk treatment

3.3. To what extent identified risks are avoided, reduced, transferred or accepted?

Implementation of controls

3.4. To what extent identified risks are controlled through preventing, deterring and detecting measures? For example, do you screen employees at the recruiting phase?

Risk follow-up

3.5. How often you update risk profiles?

Monitoring and detection, red flags

3.6. Do you monitor your employees, if they have undeclared involvement in companies, erratic behaviour (excessive gambling, misuse of alcohol) or misuse of expenses?

3.7. Do you monitor transactions, i.e. do you have payments to tax havens, tied suppliers, sales at excessive discounts?

3.8. Do you monitor your systems? For example, is there systematic abuse of procedures, unusual emails, misuse of passwords?

3.9. Do you audit corporate level risks? Are there over-zealous acquisitions strategies, artificial barriers put up by directors to avoid questions, increased concerns raised by regulators or weak management?

3.10 To what extent your company uses processes designed to detect, investigate and resolve proactively potentially significant fraud? For example use of fraud detection tests.

Managing incidents and follow up

Incident management and reporting system

4.1. In what ways fraud incidents are managed and reported in your company?

4.2. What would be the most severe fraud impact to your company?

4.3. What kind of impact creates, according to your opinion, most significant threat to your company, tangible or intangible costs?

Fraud response plan

4.4. Does your company have a fraud response plan?

Qualified investigation team

4.5. Which kind of authorities you contact when a fraud incident is revealed?

4.6. Do you have internal fraud investigation team?

Follow-up and sanctions

4.7. What kind of sanctions is used to punish fraudsters?

System follow-up and recovery

4.8. How fraud could affect your systems and what kind of measures should be done in order to recover from the losses fraud incident caused?

Management review of incidents

4.9. What kind of measures is taken in order to enhance company's ability to manage fraud risks?

INDEX OF TABLES AND FIGURES